No. _____

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

PETITION FOR WRIT OF CERTIORARI

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

QUESTION PRESENTED

When Petitioner Derrick Williams arrived from Europe at Denver International Airport, government agents seized his laptop, used forensic software to break the password and copy its data bit-for-bit, and then searched the files. The agents had neither a warrant nor suspicion that Mr. Williams was inadmissible, smuggling contraband, or evading customs duties. The question presented is:

To conduct a warrantless forensic search of a digital device at the border, do government agents need reasonable suspicion that the device contains digital contraband (as the Ninth Circuit requires), reasonable suspicion that the device contains evidence of a particular crime with a nexus to the purposes of the border search exception to the warrant requirement (as the Fourth Circuit requires), reasonable suspicion of any kind of criminal activity (which suffices in the Tenth Circuit), or no suspicion whatsoever (as the Eleventh Circuit permits)?

PARTIES TO THE PROCEEDING AND RULE 29.6 STATEMENT

The parties to the proceeding below were Petitioner Derrick Lucius Williams, Jr., and Respondent the United States of America. There are no nongovernmental corporate parties requiring a disclosure statement under Supreme Court Rule 29.6.

RELATED PROCEEDINGS

United States District Court (D. Colo.):

United States v. Derrick Lucius Williams Jr., No. 1:16-cr-00249-WJM (Sept. 25, 2017)

United States Court of Appeals (10th Cir.):

United States v. Derrick Lucius Williams, Jr., No. 18-1299 (Nov. 14, 2019)

TABLE OF CONTENTS

TABLE OF CONTENTS
(continued)

Page

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES
(continued)

Page(s)

CONSTITUTIONAL AND STATUTORY AUTHORITIES

OTHER AUTHORITIES

TABLE OF AUTHORITIES
(continued)

Page(s)

INTRODUCTION

This case presents an ideal vehicle to resolve a four-way circuit split on an issue of exceptional importance to millions of Americans.

Citizens returning from abroad know that some of their freedoms are curtailed as they cross the border. After all, "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004). So travelers may expect routine searches without any suspicion. *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985).

But nearly all Americans carry cell phones—some everywhere they go—and many travel with laptops. Surely they would be surprised that border agents might "rummage through" their electronic devices "in an unrestrained search for evidence of criminal activity." *Riley v. California*, 573 U.S. 373, 403 (2014). Indeed, when British officers took such an approach to the Founding generation's homes, they "helped spark the Revolution itself." *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018). And "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house," because from his digital devices "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions," not to mention the "picture messages, text messages, Internet browsing history," "calendars, tape recorders, libraries, diaries, albums," and more that such devices contain. *Riley*, 573 U.S. at 393–94.

An American flying into Seattle or Los Angeles from a trip abroad can deplane with little worry: Government agents may forensically search his laptop or smartphone only if they reasonably suspect that it contains digital contraband, like child pornography. They may not simply download all his files and scrutinize them for evidence of criminal activity, whether or not related to the government's interest in keeping contraband from crossing the border. *United States v. Cano*, 934 F.3d 1002, 1007, 1020 (9th Cir. 2019).

If the traveler lands at Reagan or BWI, the rules are different. Agents may forensically search his laptop or smartphone if they have reasonable suspicion that it contains evidence of a particular crime with a nexus to the purposes of the border search exception to the Fourth Amendment's usual warrant requirement. In other words, they can look for evidence of particular border-related crimes, not just contraband. *See United States v. Aigbekaen*, 943 F.3d 713, 720–23 (4th Cir. 2019).

If the traveler arrives in Denver or Salt Lake City, the rules are even more lax. In the Tenth Circuit, reasonable suspicion of criminal activity—even if untethered to digital contraband or the border search exception's purposes—is all it takes for officers to copy his digital data and analyze it six ways to Sunday, as Petitioner Derrick Williams discovered here. App. 6a–9a.

But any traveler who values his privacy should really avoid entering the country via Miami or Atlanta. In the Eleventh Circuit, every computer or cell phone is no different than a suitcase. Officers can rummage at will through an individual's private digital life with no suspicion whatsoever. *United States v. Touset*, 890 F.3d 1227, 1229, 1233–34 (11th Cir. 2018).

The courts of appeals disagree vigorously about the correct rule. In twelve opinions—both majority and separate—judges have articulated every conceivable view on the question presented. Given that hundreds of millions of people cross the border each year—most of them with digital devices—this Court should not wait any longer to answer the pressing question presented.

OPINIONS BELOW

The court of appeals' opinion is reported at 942 F.3d 1187 and reproduced at App. 1a–9a. The district court's opinion is unpublished but available at 2017 WL 11491959 and reproduced at App. 10a–38a.

JURISDICTION

The court of appeals affirmed the district court's judgment on November 14, 2019. App 1a, 9a. On January 31, 2020, Justice Sotomayor extended the time to file this petition until April 13, 2020. This Court has jurisdiction under 28 U.S.C. § 1254(1).

CONSTITUTIONAL PROVISION INVOLVED

The Fourth Amendment to the United States Constitution provides in relevant part:

> 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.

STATEMENT OF THE CASE

1. The Fourth Amendment protects against "unreasonable searches and seizures." U.S. Const. amend. IV. Ordinarily, government searches to uncover criminal wrongdoing require a warrant supported by probable cause. *Riley*, 573 U.S. at 382. "In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement." *Id.*

a. One exception applies at the border (or its functional equivalent). *Montoya de Hernandez*, 473 U.S. at 538. At the border, agents need neither a warrant nor suspicion of criminal activity to conduct routine searches. *Id.* That exception reflects "the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country." *United States v. Ramsey*, 431 U.S. 606, 620 (1977). It acknowledges the government's interests in "preventing the entry of unwanted persons and effects," *Flores-Montano*, 541 U.S. at 152, "regulat[ing] the collection of duties," and "prevent[ing] the introduction of contraband," *Montoya de Hernandez*, 473 U.S. at 537.

But the border exception is not unlimited. That is because the Fourth Amendment's "ultimate touchstone" is "reasonableness." *Riley*, 573 U.S. at 381. Thus, courts must balance the defendant's "Fourth Amendment rights" "against the sovereign's interests at the border." *Montoya de Hernandez*, 473 U.S. at 539. Indeed, in *Montoya de Hernandez* the Court held that "the detention of a traveler at the border, beyond the scope of a routine customs search and inspection"—overnight detention to see if a bowel movement would produce drugs—must be "justified" by "reasonabl[e] susp[icion] that the traveler is smuggling contraband

in her alimentary canal." *Id.* at 541. The Court so held even though the "longstanding concern for the protection of the integrity of the border" was "heightened by the veritable national crisis in law enforcement caused by smuggling of illicit narcotics." *Id.* at 538.

By contrast, in *Flores-Montano* the Court held that reasonable suspicion was not required for a border search of a vehicle's gas tank that revealed marijuana. 541 U.S. at 150. The Court explained "the reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of a person—dignity and privacy interests of the person being searched—simply do not carry over to vehicles." *Id.* at 152. Emphasizing "[t]he Government's interest in preventing the entry of unwanted persons and effects," the Court noted the thousands of "vehicle drug seizures at the southern California ports of entry" over the preceding 5½ years. *Id.* at 152–53. And the Court reasoned that "[i]t is difficult to imagine how the search of a gas tank, which should be solely a repository for fuel, could be more of an invasion of privacy than the search of the automobile's passenger compartment." *Id.* at 154.

b. Warrantless searches are reasonable only if tethered to "the justifications underlying" the particular exception to the warrant requirement. *Arizona v. Gant*, 556 U.S. 332, 343 (2009). And what may be justifiable in the case of traditional property may not extend to the electronic devices of our digital age. In *Riley*, the Court held that, despite the traditional exception allowing warrantless searches incident to arrest, officers must obtain a warrant to search digital information on a cell phone seized from an arrestee. 573 U.S. at 378, 403. The Court observed that while the

Fourth Amendment permits warrantless searches incident to arrest given "concerns for officer safety and evidence preservation," neither of those rationales applies to searches of digital data. *Id.* at 384. Digital data is not a weapon that the arrestee might use "to resist arrest or effect his escape," "[a]nd once law enforcement officers have secured a cell phone, there is no longer any risk that the arrestee himself will be able to delete incriminating data from the phone." *Id.* at 388.

The Court also recognized that searching digital data on a cell phone works a "substantial additional intrusion on privacy beyond the arrest itself." *Id.* at 393. Treating digital searches like searches of physical items "is like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Id.* The Court explained: "Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person" given their "immense storage capacity" and the types of information they hold. *Id.* Digital data on cell phones "could reveal an individual's private interests or concerns" and "where a person has been," and "can form a revealing montage of the user's life," more so than even the items in a person's home. *Id.* at 395–96.

c. This case lies at the intersection of those two lines of authority and asks what level of suspicion government agents need to forensically search the digital devices travelers carry across our borders many times each day.

2. The material facts are undisputed. Derrick Williams is a U.S. citizen and military veteran originally from Detroit. In November 2015, Mr. Williams'

flight from Paris landed at Denver International Airport. His arrival triggered "lookout" alerts in the U.S. Customs and Border Protection (CBP) computer system. App. 2a. The alerts instructed officers to send Mr. Williams to secondary screening, where he was met by a Department of Homeland Security Agent, Kyle Allen. Without a warrant or any suspicion that Mr. Williams was inadmissible, transporting contraband, or evading customs duties, Agent Allen seized Mr. Williams' laptop and sent it to an offsite lab. There, a forensic expert used software to hack into the laptop and copy all of its data. A week after the initial seizure, an agent combing through the data on the laptop discovered child pornography. This case asks whether the search of Mr. Williams' laptop was constitutional.

a. Agent Allen began investigating Mr. Williams in response to an FBI letter he received months before Mr. Williams landed in Denver. The letter stated that German police had arrested Mr. Williams for possessing a "bow/arrow and air gun." App. 11a. The letter also said that German authorities were unsure how Mr. Williams entered Germany. Back in 2011, Mr. Williams had overstayed his German visa and been banned for five years from entering Germany and other Schengen countries. During his 2015 arrest in Germany, Mr. Williams admitted that he had traveled through several Schengen member states and was planning to visit Morocco next. App. 3a.

Agent Allen did some more sleuthing. He discovered that Mr. Williams had prior state-court convictions for some nonviolent and non-drug-related crimes, including trespass, unlawful use of a financial instrument, fraud, and escape from a community-corrections sentence. *Id.*

b. Mr. Williams landed in Denver in November 2015, less than two weeks after horrific terrorist attacks in Paris. Those attacks had prompted Agent Allen to review his open investigations, including his investigation of Mr. Williams. Though nothing linked Mr. Williams to terrorist activity in any way, Agent Allen placed a CBP lookout on Mr. Williams. App. 2a–4a.

The day of Mr. Williams' flight, Agent Allen went to the airport with two computer specialists prepared to search any electronic devices Mr. Williams might have. Agent Allen had decided he was "going to search [any] electronics no matter what." R. vol. II at 110.

At the initial inspection point, Mr. Williams submitted a signed declaration form accurately reporting that he was not carrying any unlawful goods, or goods that might require the payment of duties. In the space for "Countries visited on this trip," he listed Belgium, France, and Morocco. App. 4a. Based on Agent Allen's lookout alert, the agent at the primary inspection point took Mr. Williams to Agent Allen for additional screening. App. 2a–3a.

There, agents searched Mr. Williams' luggage. They found nothing illegal, taxable, or suspicious. Agents also seized Mr. Williams' laptop and smartphone. The forensic specialists accompanying Agent Allen tried unsuccessfully to crack the passwords to those devices. *Id.*

Meanwhile, Agent Allen and a local law enforcement officer interrogated Mr. Williams. They asked him why he had traveled abroad. Mr. Williams explained that he went to marry a woman in Morocco. Because he was allowed to stay in Morocco for only three months at a time, when those first three months

were up he traveled to Belgium and stayed there until he could return to Morocco. He married the woman on his second trip to Morocco. App. 15a–16a.

The officers also asked Mr. Williams for the passwords to his laptop and phone. He refused, stating that searching those devices would be an invasion of his privacy. The officers told Mr. Williams they would keep the devices and asked him where they should be returned. The address he gave was different from the address he had listed on his customs form. The officers did not follow up on the discrepancy.

The officers next asked Mr. Williams about the terrorist attacks in Paris. Mr. Williams denounced the terrorists as "fake Muslims" whose actions were "totally against what Islam is about." Gov't Ex. 10 at 19:35–20:05. He told the officers he had been in Paris for only a few days, and not when the attacks occurred.

Finally, the officers asked Mr. Williams about his travels in Germany. They repeatedly asked if he had been there in the past six months. Mr. Williams did not give a straight answer. The officers then allowed Mr. Williams to enter the country. App. 5a.

c. The next day, Agent Allen took Mr. Williams' laptop and phone to a lab where forensic specialists began their work. They first removed the computer's hard drive and attached it to a Tableua SATA write-protection device. They then used forensic software, EnCase 7.10, to hack into the hard drive. R. vol. II at 137–38. The specialists then copied "[e]very bit of binary information" onto a government hard drive, including Mr. Williams' emails, search history, and even deleted files. *Id.* at 120. In addition, the software created a forensic disk image, interpreted the data, and

reconstructed it onto a forensic analysis platform. This process took "most of [a] day." *Id.* at 140.

The specialists were unable to break the encryption on Mr. Williams' smartphone. But eventually a different government lab was able to search the phone. Analysts found nothing illegal. App. 22a.

The agents waited five more days before searching the laptop again. Eventually, using the forensic software and the forensic analysis platform, an agent searching the data on the laptop discovered child pornography. The agent paused the search. Two days later, after obtaining a warrant, agents uncovered more images and videos of child pornography. App. 5a.

3. The government indicted Mr. Williams on one count of transporting child pornography and one count of possessing child pornography. App. 10a. Mr. Williams moved to suppress the evidence from his laptop. He acknowledged that under the border exception to the warrant requirement, agents may generally conduct routine searches at the border without any suspicion. He argued, however, that an intrusive search of personal electronic devices could be conducted only if the agents had reasonable suspicion tethered to one of the border search exception's purposes. Mr. Williams argued that the search of his laptop was unconstitutional because it was "completely disconnected from the considerations underlying the breadth of the government's authority to search at the border." R. vol. I at 168; *see id.* at 28–30, 159–63, 192–93. He also argued that the second search (after the warrant was issued) was tainted by the first.

The district court denied the suppression motion. App. 10a–11a. The court assumed that the search required reasonable suspicion. But, the court concluded, the reasonable suspicion could be of any criminal activity; it did not have to relate to a particular offense. App. 32a. And based on Mr. Williams' behavior, the court held, the officers had reasonable suspicion that Mr. Williams was engaged in some sort of illegal conduct. App. 35a.

Mr. Williams conditionally pleaded guilty, reserving his right to appeal the denial of his suppression motion. He was sentenced to 84 months in prison and five years of supervised release. App. 2a.

4. The Tenth Circuit affirmed. The court "decline[d]" to "find that searches of personal electronic devices at the border must be supported by reasonable suspicion." App. 6a. Instead, the court thought "that reasonable suspicion was present here." *Id.* Though the court never identified a particular crime the officers might have reasonably suspected, the court listed four circumstances it thought gave rise to reasonable suspicion of some sort of criminal activity. *First*, Mr. Williams had "fled the United States a fugitive," been banned from entering Germany, and defied the German travel ban. App. 7a. *Second*, he did not list Germany on his customs form and "evaded all of Agent Allen's questions regarding his time in Germany." *Id.* *Third*, Mr. Williams traveled on a one-way ticket and visited three countries (Belgium, France, and Morocco) "intimately linked to the attacks" in Paris. App. 8a. *Fourth*, when asked where he wanted his electronics sent, Mr. Williams gave a different address than the one listed on his customs form. *Id.*

The court of appeals rejected Mr. Williams' argument that the agents' suspicion "was not particularized enough to justify the search." *Id.* Mr. Williams explained that, "because border agents did not suspect him of" violating the laws "that border agents are tasked exclusively with upholding," *i.e.*, "customs laws and [laws against] the importation of contraband," they could not search his electronic devices. *Id.* The court "disagree[d] because the Fourth Amendment does not require law enforcement officers to close their eyes to suspicious circumstances." *Id.*

REASONS FOR GRANTING THE WRIT

I. The courts of appeals are split four ways on the suspicion required for a forensic search of an electronic device at the border

The courts of appeals have divided four ways on the kind of suspicion required for a warrantless border search of digital data, with separate opinions expressing still additional views. The Ninth Circuit, over two dissents, requires reasonable suspicion that an electronic device contains digital contraband. The Fourth Circuit, disagreeing with two separate opinions, requires individualized suspicion that the 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." *Aigbekaen*, 943 F.3d at 721. The Tenth Circuit below held that reasonable suspicion of *any* criminal activity suffices. And the Eleventh Circuit requires no suspicion whatsoever—despite two separate opinions, one concluding that officers must get a warrant.

The split is outcome-determinative here, as it will be in most cases. Had Mr. Williams landed in San Francisco, the search would have been unconstitutional because the Ninth Circuit requires reasonable suspicion that the device to be forensically searched contains digital contraband—suspicion the agents did not have. In fact, the court below did not identify *any* particular crime of which agents supposedly had suspicion, even though "the Fourth Amendment requires … an individualized suspicion that a particular citizen was engaged *in a particular crime*." *Kansas v. Glover*, No. 18-556, 2020 WL 1668283, at *5 n.1 (U.S. Apr. 6, 2020) (emphasis added). Similarly, had Mr. Williams landed at Reagan, the search would have been unconstitutional because nothing Mr. Williams was supposedly suspected of doing had any nexus to the border search exception's purposes. But because the search occurred in the Tenth Circuit, it was deemed constitutional since the officers supposedly had reasonable suspicion that some unspecified criminal activity was afoot. The search would also have been constitutional in the Eleventh Circuit because there officers need no suspicion at all.

This circuit split makes for a perfect cert candidate. Not only is the split outcome determinative, but it reflects every possible view on the question presented, and the lower courts recognize their disagreement and have called for this Court's guidance.

A. The Ninth Circuit requires reasonable suspicion that the electronic device contains digital contraband

In *United States v. Cotterman*, 709 F.3d 952, 967–68 (9th Cir. 2013) (en banc), the en banc Ninth Circuit held that the forensic examination of a laptop seized

at the border requires reasonable suspicion. And in *Cano*, Judge Bybee, writing for the court, "clarif[ied] *Cotterman* by holding that … cell phone searches at the border, whether manual or forensic, must be limited in scope to a search for digital contraband." 934 F.3d at 1007. Thus, "border officials may conduct a forensic cell phone search only when they reasonably suspect that the cell phone contains contraband." *Id.* at 1020. Had Mr. Williams landed in the Ninth Circuit, the forensic search would have been unconstitutional because the agents did not reasonably suspect that the laptop contained contraband.

1. a. In *Cotterman*, the Ninth Circuit held that a forensic border laptop search requires reasonable suspicion. 709 F.3d at 968. There, agents seized the defendant's "laptop at the U.S.–Mexico border in response to an alert based in part on a fifteen-year-old conviction for child molestation." *Id.* at 956. A forensic search revealed child pornography. *Id.* at 958.

The Ninth Circuit acknowledged that "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *Id.* at 960 (quoting *Flores-Montano*, 541 U.S. at 152). But given "the expectation of privacy … with respect to the gigabytes of data regularly maintained as private and confidential on digital devices," *id.* at 957, the court reasoned, the government's interest "does not mean … that at the border anything goes," *id.* at 960.

"Electronic devices are capable of storing warehouses full of information"—far beyond the capacity even of "a car full of packed suitcases with sensitive documents." *Id.* at 964. These devices, the court explained, also "contain the most intimate details of our

lives: financial records, confidential business documents, medical records and private emails." *Id.* In the court's view, "[a] person's digital life ought not be hijacked simply by crossing a border." *Id.* at 965. Yet a forensic examination of a laptop is "essentially a computer strip search" that "intrudes upon privacy and dignity interests to a far greater degree than a cursory search at the border." *Id.* at 966. Given the "substantial intrusion upon personal privacy and dignity" wrought by a forensic digital search, *id.* at 967, the court held that the Fourth Amendment requires "a particularized and objective basis for suspecting the particular person stopped of criminal activity," *id.* at 968.

b. Judge Callahan dissented in relevant part. She thought the majority's holding "flout[ed] more than a century of Supreme Court precedent, [was] unworkable and unnecessary, and [would] severely hamstring the government's ability to protect our borders." *Id.* at 971 (Callahan, J., concurring in part, dissenting in part, and concurring in the judgment). At the border, she reasoned, the government's strong security interests make "searches of people and their property … *per se* reasonable." *Id.* "The fact that electronic devices are capable of storing a lot of personal information does not make an extensive search of them 'particularly offensive,'" she opined. *Id.* at 977 (quoting *Flores-Montano*, 541 U.S. at 154 n.2). She warned that "the majority's new limits … will make it much harder for border agents to do their jobs." *Id.* at 979.

c. Judge Milan Smith also dissented. *Id.* at 981–88 (M. Smith, J., dissenting). In his view, the en banc decision left border agents "to divine on an ad hoc ba-

sis whether a property search is sufficiently 'comprehensive and intrusive' to require reasonable suspicion." *Id.* at 981. He protested that "the majority opinion makes such a legal bouillabaisse out of the previously unambiguous border search doctrine, that [he] sincerely hope[d] the Supreme Court will grant certiorari." *Id.*

2. In *Cano*, the Ninth Circuit built on *Cotterman*, holding that "cell phone searches at the border, whether manual or forensic, must be limited in scope to a search for digital contraband." 934 F.3d at 1007. Writing for the court, Judge Bybee explained that forensic searches must be based on reasonable suspicion that the device contains digital contraband. *Id.* at 1020. There, border agents arrested the defendant when a dog sniff alerted them to cocaine in his vehicle's spare tire. *Id.* at 1008. After manually searching the phone, agents used forensic software to download its data. *Id.* at 1008–09.

The Ninth Circuit held that the forensic search and one of the manual searches violated the Fourth Amendment. The court explained that border searches, as exceptions to the warrant requirement, "are subject to two important constraints": (1) searches "must be within the *scope* of the exception" and (2) searches that are sufficiently "*intrusive* … require additional justification, up to and including probable cause and a warrant." *Id.* at 1010–11. On the second point, the Ninth Circuit extended to cell phones *Cotterman*'s requirement of reasonable suspicion to search laptops. *Id.* at 1014. The court observed that in *Cotterman* it had "anticipated the Supreme Court's reasoning in *Riley*," and that it could "find no basis to distinguish a forensic cell phone search from

a forensic laptop search." *Id.* at 1015. The court noted, however, that in the intervening years "the Eleventh Circuit disagreed with *Cotterman*," instead holding "that no level of suspicion was required to conduct a forensic search of a cell phone." *Id.* at 1015 n.8.

On the first point, the Ninth Circuit held that the "exception authorizes warrantless searches of a cell phone only to determine whether the phone contains contraband," *not* "search[es] for evidence of border-related crimes." *Id.* at 1017–18; *see id.* at 1013–14. Although border officials may seize contraband, the court reasoned, they "have no general authority to search for crime," "even if there is a possibility that such crimes may be perpetrated at the border in the future." *Id.* at 1017. The court explained that the border search exception could not extend beyond the historic rationale of locating contraband to searching for evidence. *Id.* at 1018 (quoting *Boyd v. United States*, 116 U.S. 616, 623 (1886), *overruled in part on other grounds by Warden v. Hayden*, 387 U.S. 294 (1967)).

The Ninth Circuit recognized its disagreement "with the Fourth Circuit's decision in" *United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018). *Cano*, 934 F.3d at 1017. In *Kolsuz*, the Fourth Circuit held that "the justification behind the border search exception is broad enough to accommodate not only the direct interception of contraband as it crosses the border"—as far as the Ninth Circuit would go—but also "the power to search for *evidence* of contraband that is *not* present at the border." *Id.* at 1017–18 (explaining *Kolsuz*).

B. The Fourth Circuit requires reasonable suspicion that the forensic search will reveal contraband or evidence of a crime with a nexus to the purposes of the border search exception

Border officials need reasonable suspicion to conduct a forensic search of digital data in the Fourth Circuit too. But reasonable suspicion isn't limited to digital contraband. Agents may search for evidence based on "individualized suspicion of an offense that bears some 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." *Aigbekaen*, 943 F.3d at 721. Had Mr. Williams landed in the Fourth Circuit, the search would have been unconstitutional because the agents didn't reasonably suspect that they would find evidence of any crime with such a nexus. Indeed, the Tenth Circuit didn't articulate reasonable suspicion of any particular crime at all. *See* App. 7a–8a.

1. a. In *Kolsuz*, the Fourth Circuit held that a forensic search of a smartphone at the border is a nonroutine search "requiring some measure of individualized suspicion." 890 F.3d at 137. There, agents arrested the defendant as he was attempting to board a flight to Turkey after finding firearms parts for which he lacked an export license in his luggage. *Id.* at 136–39. The agents eventually conducted a forensic search of the defendant's iPhone. *Id.* at 139.

The Fourth Circuit reasoned, "As a general rule, the scope of a warrant exception should be defined by its justifications." *Id.* at 143. But, the court noted, the agents "reasonably believed that their search would

reveal not only evidence of the export violation they already had detected, but also information related to other ongoing attempts to export illegally various firearms parts." *Id.* That suspicion, in other words, was of "a transnational offense that goes to the heart of the border search exception, which rests in part on the sovereign interest of protecting and monitoring exports from the country." *Id.*

The Fourth Circuit then concluded that "a forensic border search of a phone must be treated as nonroutine, permissible only on a showing of individualized suspicion." *Id.* at 144. Discussing *Riley*, the court reasoned that "[t]he sheer quantity of data stored on smartphones and other digital devices dwarfs the amount of personal information that can be carried over a border—and thus subjected to a routine border search—in luggage or a car." *Id.* at 145. And, it reasoned, "[t]he uniquely sensitive nature of that information matters." *Id.*

b. Judge Wilkinson concurred only in the judgment. In his view, "[t]he standard of reasonableness in the particular context of a border search should be principally a legislative question, not a judicial one." *Id.* at 148 (Wilkinson, J., concurring in the judgment). He pointed to the government's "powerful" interests at the border and opined that setting a constitutional "floor" is "a hugely consequential policy judgment" better left to "the legislative process." *Id.* at 151.

2. a. The Fourth Circuit applied *Kolsuz* in *Aigbekaen*, concluding that warrantless forensic searches of a laptop, iPhone, and iPod turning up child pornography violated the Fourth Amendment because the agents had reasonable suspicion only that the defendant "had previously committed grave *domestic*

crimes," *i.e.*, sex trafficking. 943 F.3d at 720–23. "[T]o conduct such an intrusive and nonroutine search under the border search exception," the court reiterated, "the Government must have individualized suspicion of an offense that bears some 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." *Id.* at 721. The court did "not question the import of the Government's general interest in combatting crime." *Id.* at 722. But that generalized interest cannot "eclipse[] individuals' privacy interests in the vast troves of data contained on their digital devices when the suspected offenses have little or nothing to do with the border." *Id.* The court explained that "suspicion that [a] phone may contain evidence of any prior domestic crime" does not trigger the border search exception. *Id.* at 723.

The Fourth Circuit also rejected the government's argument that suspicion of sex trafficking sufficed simply because it "commonly involv[es] cross-border movements." *Id.* at 721. The court explained that officers must have "*individualized* suspicion" that the crime "in the individual case at hand" has a "transnational component" tethered to the border search exception's purposes. *Id.*

b. Judge Richardson concurred only in the judgment, opining that the majority's "'nexus' test … is in deep tension with Supreme Court precedent." *Id.* at 726 (Richardson, J., concurring in the judgment). In his view, "[t]he Supreme Court has limited the border-search doctrine only when the *intrusiveness* of the search makes it unreasonable without particularized suspicion," whereas the majority's nexus requirement

turned instead on "the nature of the *government's interests* at stake." *Id.* at 730. Thus, although he found "historical support" for the Ninth Circuit's view that "the border-search doctrine is concerned solely with detection of contraband," he thought "lower-court judges" powerless to "rewrite" the law. *Id.* at 730–31. Judge Richardson also dismissed the majority's reliance on *Riley* because it "concerned the far different context of searches incident to arrest" and because it focused on "the *type of search*—not the *suspicion* motivating the search." *Id.*

C. In the Tenth Circuit, reasonable suspicion of any criminal activity suffices

In this case, the Tenth Circuit cursorily rejected Mr. Williams' argument that "because border agents did not suspect him" of crimes involving the customs laws or contraband, "they were prevented from searching his laptop and cell phone." App. 8a. The court stated only that it "disagree[d] because the Fourth Amendment does not require law enforcement officers to close their eyes to suspicious circumstances." *Id.* (cleaned up). The reasonable suspicion it found turned on (1) "Mr. Williams's criminal history concern[ing] border offenses"—apparently his unlawful time in Germany; (2) his failure to disclose that he had traveled to Germany; (3) his return "on a one-way ticket originating in Paris—the site of devastating terrorist attacks less than two weeks earlier"; and (4) the discrepancy between the address he wrote on the customs form and the address to which he wanted his electronics returned. App. 7a–8a.

What crime it thought that added up to, the Tenth Circuit didn't say. Unlike the Ninth Circuit, the Tenth

Circuit didn't require reasonable suspicion of digital contraband (and there was no such suspicion). And unlike the Fourth Circuit, it didn't require reasonable suspicion of evidence of a particular crime with a nexus to the border search exception's purposes (and, once again, there was no such suspicion).

D. The Eleventh Circuit requires no suspicion whatsoever

The Eleventh Circuit requires no suspicion or nexus whatsoever for border searches of digital devices. The court first rejected a warrant requirement in *United States v. Vergara*, 884 F.3d 1309, 1311 (11th Cir. 2018), over a vigorous dissent by Judge Jill Pryor. It then rejected reasonable suspicion in *Touset*. 890 F.3d at 1229, 1233–34. Thus, had Mr. Williams landed in Miami, the search of his laptop would have passed constitutional muster.

1. a. In *Vergara*, a divided panel of the Eleventh Circuit, in an opinion by Judge William Pryor, held that "border searches never require a warrant or probable cause." 884 F.3d at 1311. The court therefore rejected the defendant's argument that the trial court should have suppressed child pornography discovered during warrantless forensic searches of his phones. *Id.* at 1312–13. This Court's decision in *Riley* did "not change this rule," the panel majority reasoned, because the Court there stated that "'even though [the search-incident-to-arrest exception] does not apply to cell phones, other case-specific exceptions may still justify a warrantless search of a particular phone.'" *Id.* (quoting *Riley*, 573 U.S. at 401–02).

b. Judge Jill Pryor dissented. "[P]redict[ing] how the Supreme Court would balance the interests" given

this Court's recognition in *Riley* of "the significant privacy interests implicated in cell phone searches," she concluded that "a forensic search of a cell phone at the border requires a warrant supported by probable cause." *Id.* at 1313 (J. Pryor, J., dissenting). She explained that "the privacy interests implicated in *forensic* searches are even greater than those involved in the manual searches at issue in *Riley*," which involved devices "fundamentally different from any object traditionally subject to government search at the border." *Id.* at 1315. "Before cell phones," Judge Pryor observed, "border searches were limited by 'physical realities' that ensured any search would impose a relatively narrow intrusion on privacy," *id.*, whereas "a cell phone search 'typically expose[s] to the government far *more* than the most exhaustive search of a house,'" *id.* at 1316 (quoting *Riley*, 573 U.S. at 396). That is especially true in the case of forensic searches, which are "experts' work, performed by a trained analyst at a government forensics laboratory." *Id.*

Judge Pryor next reasoned that "the rationales underlying the border search exception lose force when applied to forensic cell phone searches." *Id.* at 1317. For starters, "cell phones do not contain the physical contraband that border searches traditionally have prevented from crossing the border, 'whether that be communicable diseases, narcotics, or explosives.'" *Id.* (quoting *Montoya de Hernandez*, 473 U.S. at 544). And "electronic contraband is borderless and can be accessed and viewed in the United States without ever having crossed a physical border." *Id.* In Judge Pryor's view, the possibility that "forensically searching a cell phone may lead to the discovery of

physical contraband" already "inside the border" presents only a "general law enforcement justification … quite far removed from the purpose originally underlying the border search exception." *Id.*

Judge Pryor also criticized the majority's cramped view of *Riley*. Contrary to the majority's claim, she explained, this Court's reservation of "other case-specific exceptions [that] may still justify a warrantless search" referred to "extreme hypotheticals" concerning immediate danger that could thus trigger the exigent circumstances exception to the warrant requirement. *Id.* at 1318 (quoting *Riley*, 573 U.S. at 402).

2. a. Shortly after *Vergara*, a divided panel of the Eleventh Circuit, in another opinion by Judge William Pryor, concluded that "the Fourth Amendment does not require any suspicion for forensic searches of electronic devices at the border." *Touset*, 890 F.3d at 1231. *Touset* involved forensic searches of laptops and external hard drives that revealed child pornography. *Id.* at 1230. The border agents were acting on a "lookout" based on a "series of investigations by private organizations and the government [that] suggested that [the defendant] was involved with child pornography." *Id.* Despite concluding that the agents had reasonable suspicion that the defendant had child pornography on the devices, *id.* at 1237–38, the court took the additional step of holding that no suspicion was required anyway, *id.* at 1232–37.

The Eleventh Circuit reasoned that although this Court "required reasonable suspicion for the prolonged detention of a *person*" in *Montoya de Hernandez*, it "has never required reasonable suspicion for a search of property at the border." *Id.* at 1233. The panel found "no reason why the Fourth Amendment

would require reasonable suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property." *Id.* In the majority's view, questions about the intrusiveness or indignity of a search were relevant only to a search of *the body*. *Id.* at 1234.

The Eleventh Circuit acknowledged that it disagreed with "the Fourth and the Ninth Circuits." *Id.* Those courts were wrong, it opined, because this Court rejected a routine–nonroutine distinction in *Flores-Montano*, and nothing in *Riley* was relevant. *Id.* (citing 541 U.S. at 152). And, the majority continued, "the Fourth Amendment does not guarantee the right to travel without great inconvenience." *Id.* at 1235. The court further reasoned that "digital child pornography poses the same exact risk of unlawful entry at the border as its physical counterpart," and that "requir[ing] reasonable suspicion for searches of electronic devices … would create special protection for the property most often used to store and disseminate child pornography." *Id.* The panel concluded that courts "must allow Congress to design the appropriate standard 'through the more adaptable legislative process and the wider lens of legislative hearings.'" *Id.* at 1237 (quoting *Kolsuz*, 890 F.3d at 150 (Wilkinson, J., concurring in the judgment)).

b. Judge Corrigan (M.D. Fla., by designation) did not join the panel majority's holding that no suspicion is required. *See id.* at 1238 (Corrigan, J., concurring in part and concurring in the judgment). "In the district court," he explained, "the government agreed that the applicable Fourth Amendment test was whether there was reasonable suspicion." *Id.* And

the court did not need to reach the issue given its holding that agents had reasonable suspicion. *Id.* at 1239.

* * *

In sum, the courts of appeals have divided four ways on the question presented, with jurists taking every position imaginable in 12 different opinions. They have opined that the answer is simple—get a warrant (J. Pryor, J.); that agents may search only on reasonable suspicion of contraband (9th Cir.); that agents may search on reasonable suspicion of evidence of a particular crime with a nexus to the border search exception's purposes (4th Cir.); that agents may search on reasonable suspicion of *any* criminal activity (10th Cir.); that agents don't need any suspicion at all (11th Cir.); or that whatever suspicion is required is a question for Congress (Wilkinson, J.). The question presented is outcome-determinative here, as it will be in many cases. And further percolation will not clarify the issue or suggest alternative approaches. Lower courts, travelers, and border agents all urgently need this Court's guidance now on this important question.

II. The question presented is exceptionally important

This Court's 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." *Vergara*, 884 F.3d at 1318 (J. Pryor, J., dissenting). The question implicates both the government's interest in protecting our borders and individuals' interest in remaining free from unreasonable searches. And given the frequency with which the question arises—hundreds of millions of people cross

our borders each year—this Court's guidance is urgently needed.

A. To be sure, "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *Flores-Montano*, 541 U.S. at 152. "Porous borders are uniquely tempting to those intent upon inflicting the vivid horrors of mass casualties." *Kolsuz*, 890 F.3d at 152 (Wilkinson, J., concurring in the judgment). And "there is the danger of highly classified technical information being smuggled out of this country only to go into the hands of foreign nations who do not wish us well and who seek to build their armaments to an ever more perilous state." *Id.* The government thus needs tools "to prevent smuggling and to prevent prohibited articles from entry." *Montoya de Hernandez*, 473 U.S. at 537–38.

But individuals still have a right to be free from unreasonable searches. Knowing where the government's interest must give way to the private interest is vital in this digital age. The ubiquity of digital devices—nearly every American adult has a cellphone—and of international travel—400 million travelers crossed our Nation's border in 2018—mean that border searches of these digital devices are becoming increasingly common. Clarity on when border agents can forensically search travelers' digital devices is thus vitally important to both the federal government and the hundreds of millions of people who cross our border each year.

B. Modern digital devices "differ in both a quantitative and a qualitative sense from other objects that" people once traveled with. *Riley*, 573 U.S. at 393. Today's smartphones are capable of storing "millions of

pages of text, thousands of pictures, or hundreds of videos." *Id.* at 394. Laptops can currently store more than a billion and a half pages of text or 80 days of video.[1]

As this Court has noted, this immense storage capacity has "has several interrelated consequences for privacy." *Id.* Digital devices can reveal "nearly every aspect of" a person's life—"from the mundane to the intimate." *Id.* at 395. Not only do these devices collect "in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record," they also can contain data that "date back of the purchase of the phone or even earlier." *Id.* at 394. "Smartphones and laptops contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails." *Kolsuz*, 890 F.3d at 145.

Searching these devices can cause dignitary and psychological harms. The device may contain pictures of a Muslim woman without her headscarf. *Alasaad v. Nielson*, No. 17-cv-11730, 2018 WL 2170323, at *20 (D. Mass. May 9, 2018). Or it may contain a recording of person's deepest thoughts conveyed to a therapist, so a search "invad[es] not only the subject's house but his or her thoughts as well." Craig M. Bradley, *Constitutional Protection for Private Papers*, 16 HARV. C.R.-C.L. L. REV. 461, 483 (1981). As this Court put it, searching

---

[1] *See* Apple, *Compare Mac models*, https://www.apple.com/mac/compare/ (last visited April 10, 2020); Jenia I. Turner, *Managing Digital Discovery in Criminal Cases*, 109 J. CRIM. L. & CRIMINOLOGY 237, 311 n.69 (2019).

a digital device "would typically expose to the government far *more* than the most exhaustive search of a house." *Riley*, 573 U.S. at 396.

And, of course, personal digital devices are everywhere. Cell phones are "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Id.* at 385. In the years since *Riley*, their pervasiveness has only grown. Today, nearly every American adult (96%) owns some kind of cell phone; four-fifths own a smartphone.[2] And nearly three-quarters of American adults own a computer, whether a laptop or a desktop, while about half own tablet computers.[3]

C. "[I]t is neither realistic nor reasonable to expect the average traveler to leave his digital devices at home when traveling." *Kolsuz*, 890 F.3d at 145; *see Cotterman*, 709 F.3d at 965. People "compulsively carry cell phones with them all the time." *Carpenter*, 138 S. Ct. at 2218. "According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower." *Riley*, 573 U.S. at 395. Mobile devices serve "as digital umbilical cords to what travelers leave behind at home or at work, indispensable travel accessories in their own right, and safety nets to protect against the risks of traveling abroad." *United States v. Saboonchi*, 990 F. Supp. 2d 536, 557–58 (D. Md. 2014).

---

[2] Pew Research Center, Mobil Fact Sheet (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/mobile/ (last visited April 10, 2020).

[3] *Id.*

Given the staggering number of people crossing the border each year, it's no wonder searches of these devices are on the rise. In fiscal year 2018, border agents processed more than 413 million travelers—more travelers than the entire population of the United States.[4] That is a 5.3% increase over 2017 and a 10.5% increase compared to five years before.[5]

Searches of electronic devices have increased too. In fiscal year 2017, CBP conducted 60% more searches of electronic devices than in 2016, searching approximately 30,200 devices at the border and nearly tripling the annual number of searches since 2015.[6] *See also Vergara*, 884 F.3d at 1318 (J. Pryor, J., dissenting). And travelers have filed hundreds of complaints with the Department of Homeland Security over suspicionless searches of their digital devices.[7]

The question presented is thus important to both the government and the hundreds of millions of people who enter and leave the United States. The government needs tools to protect the sovereign borders and

---

[4] CBP, *CBP Trade and Travel Report: Fiscal Year 2018*, at 1 (July 2019), https://www.cbp.gov/sites/default/files/assets/documents/2019-Jul/CBP%20FY18%20Trade%20and%20Travel%20Report-compliant.pdf (last visited April 10, 2020).

[5] *Id.*

[6] CBP, *CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics* (Jan. 5, 2018), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and (last visited April 10, 2020).

[7] Charlie Savage & Ron Nixon, *Privacy Complaints Mount Over Phone Searches at U.S. Border Since 2011*, N.Y. TIMES (Dec. 22, 2017), https://www.nytimes.com/2017/12/22/us/politics/us-border-privacy-phone-searches.html (last visited April 10, 2020).

the people within them. And individuals need protection of their right against unreasonable searches. Because the question presented lies at the intersection of national security and personal privacy and arises daily, this Court's guidance is sorely needed.

III. The Tenth Circuit's decision is wrong

The Tenth Circuit erroneously concluded that reasonable suspicion of *any* criminal activity—even if untethered to digital contraband or the border search exception's purposes—permits officers to forensically search a traveler's laptop.

First, as this Court has recognized, the Fourth Amendment may demand reasonable suspicion even at the border. *Montoya de Hernandez*, 473 U.S. at 541. The question, as always, is how to *balance* the individual's "Fourth Amendment rights" "against the sovereign's interests." *Id.* at 539.

Digital devices tip the scales. *Riley* makes clear that digital devices differ qualitatively and quantitatively from items traditionally subject to search. 573 U.S. at 393–96. They contain vast amounts of information, much of it sensitive, all in one place. *Id.* at 394. Before "the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day." *Id.* at 395. Now the vast majority of adults do. *Id.*; *supra* p. 29.

A cell phone search—particularly a forensic search—allows officers "to rummage at will among a person's private effects." *Riley*, 573 U.S. at 399 (quoting *Gant*, 556 U.S. at 345). A laptop search is no different, because laptops too "are capable of storing warehouses full of information." *Cotterman*, 709 F.3d

at 964. Such searches thus intrude deeply on an individual's "dignity and privacy interests," *Flores-Montano*, 541 U.S. at 152, for they allow the government to piece together "[t]he sum of an individual's private life," *Riley*, 573 U.S. 394. These searches are nothing like the search of a gas tank, "which should be solely a repository for fuel." *Flores-Montano*, 541 U.S. at 154. In short, equating digital searches with predigital searches is like equating a Google search with thumbing through the Yellow Pages (or a trip to the launch pad with a trip to the stables, *Riley*, 573 U.S. at 393).

Second, this Court has long recognized that exceptions to the warrant requirement extend only so far as their rationales. *See, e.g.*, *Riley*, 573 U.S. at 385–91; *Gant*, 556 U.S. at 351. The purpose of the border search exception isn't to promote law enforcement or to discover evidence of criminal behavior generally, but to "protect[] this Nation from entrants who may bring anything harmful into [it]." *Montoya de Hernandez*, 473 U.S. at 544; *Ramsey*, 431 U.S. at 606; *United States v. Molina-Isidoro*, 884 F.3d 287, 289, 295 (5th Cir. 2018) (Costa, J., specially concurring) ("[E]very border-search case the Supreme Court has decided involved searches to locate items being smuggled.").

Indeed, this Court has long distinguished between "[t]he search for and seizure of stolen or forfeited goods, or goods liable to duties," on the one hand, and "a search for and seizure of a man's private books and papers for the purpose … of using them as evidence against him." *Boyd*, 116 U.S. at 623. "The two things differ *toto coelo*," *id.*—that is, the "whole extent of the heavens," *Molina-Isidoro*, 884 F.3d at 296 (Costa, J., specially concurring). While border agents have long been authorized to search for and seize contraband,

"[n]o similar tradition exists for unlimited authority to search and seize items that might help to prove border crimes but are not themselves instrumentalities of the crime." *Id.* at 297. Because "a warrantless search … must be limited in scope to that which is justified by the particular purposes served by the exception," *Florida v. Royer*, 460 U.S. 491, 500 (1983) (opinion of White, J.), the border search exception authorizes warrantless searches of the digital data on electronic devices only on reasonable suspicion that it contains contraband.

Third, requiring reasonable suspicion of digital contraband or of evidence of a crime related to the border search exception's purposes will not throw border security into chaos. *But see Cotterman*, 709 F.3d at 981 (M. Smith, J., dissenting); *Kolsuz*, 890 F.3d at 148–49 (Wilkinson, concurring in the judgment). In fact, "as a matter of commonsense and resources, it is only when reasonable suspicion is aroused that such searches typically take place," *Cotterman*, 709 F.3d at 967 n.14—or at least it should be, *see also id.* at 968 (Callahan, J., concurring in part, dissenting in part, and concurring in the judgment) ("[B]order agents will conduct forensic electronic searches of people who … the agents reasonably suspect may be trying to carry illegal articles into … the country."). And even if requiring reasonable suspicion *would* "have an impact on the ability of law enforcement to combat crime," that is because "[p]rivacy comes at a cost." *Riley*, 573 U.S. at 401. Indeed, the rule in *Riley* applied to warrantless searches incident to arrest, even though such searches "occur with far greater frequency than searches conducted pursuant to a warrant." *Id.* at 382.

No American would be surprised to learn that government agents need an objectively good reason to search their digital devices. But most would be shocked to learn that agents may copy their hard drives bit-for-bit just because they fly in from another country and somehow seem suspicious to the agents. The Tenth Circuit erred in endorsing that approach.

IV. This case is an ideal vehicle

This case provides the Court with an ideal vehicle to decide the question presented. The facts are straightforward and undisputed, and there is no alternative holding. *Supra* pp. 6–12. The case boils down to a clear legal question: What kind of suspicion is required to search a traveler's digital devices at the border? Mr. Williams had the misfortune of landing in Denver, where agents are free to rummage through laptops if they reasonably suspect the owner of *any* criminal activity. If he had landed in Miami, he might have suffered the same fate, because agents there need no suspicion at all. But had Mr. Williams landed in Los Angeles, the forensic laptop search would have been unconstitutional because the agents lacked reasonable suspicion that it contained contraband. So too had he landed at Reagan or BWI, because the agents did not reasonably believe they would find evidence on his laptop of a crime involving threatening national security, evading duties, inadmissibility, or importing contraband.

No further percolation is necessary. The appellate courts have thoroughly aired the issue, offering this Court every conceivable legal rule. This case presents the Court with an optimal opportunity to answer the important question presented.

CONCLUSION

The Court should grant the petition for writ of certiorari.

April 13, 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