No. 19-1221

In the Supreme Court of the United States

DERRICK LUCIUS WILLIAMS, JR., PETITIONER

v.

UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE TENTH CIRCUIT

BRIEF FOR THE UNITED STATES IN OPPOSITION

NOEL J. FRANCISCO
Solicitor General
Counsel of Record
BRIAN A. BENCZKOWSKI
Assistant Attorney General
DANIEL N. LERMAN
Attorney

Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217

QUESTION PRESENTED

Whether the court of appeals correctly determined that the warrantless border search of petitioner's laptop computer was permissible under the border-search exception to the Fourth Amendment's warrant requirement.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases:

Cases—Continued: Page

Constitution, statutes, and rules:

Statutes and rules—Continued: Page

In the Supreme Court of the United States

No. 19-1221

DERRICK LUCIUS WILLIAMS, JR., PETITIONER

v.

UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE TENTH CIRCUIT

BRIEF FOR THE UNITED STATES IN OPPOSITION

OPINIONS BELOW

The opinion of the court of appeals (Pet. App. 1a-9a) is reported at 942 F.3d 1187. The order of the district court (Pet. App. 10a-38a) is not published in the Federal Supplement but is available at 2017 WL 11491959.

JURISDICTION

The judgment of the court of appeals was entered on November 14, 2019. On January 31, 2020, Justice Sotomayor extended the time within which to file a petition for a writ of certiorari to and including April 13, 2020 (Monday), and the petition was filed on that date. The jurisdiction of this Court is invoked under 28 U.S.C. 1254(1).

STATEMENT

Following a guilty plea in the United States District Court for the District of Colorado, petitioner was convicted on one count of transporting child pornography,

in violation of 18 U.S.C. 2252A(a)(1) and (b)(1), and one count of possessing child pornography, in violation of 18 U.S.C. 2252A(a)(5)(B) and (b)(2). Judgment 1. Petitioner was sentenced to 84 months of imprisonment, to be followed by five years of supervised release. Judgment 2-3. The court of appeals affirmed. Pet. App. 1a-9a.

1. a. In November 2007, petitioner, a U.S. citizen, was serving a community corrections sentence in Colorado. Pet. App. 13a. One evening, instead of reporting to work as authorized by his parole officer, petitioner fled the country, flying from Denver to Germany, where he remained for several years. *Ibid.*; see D. Ct. Doc. 27, at 5 (Apr. 21, 2017); D. Ct. Doc. 27-3, at 2-3. Petitioner's passport expired in 2008, but he remained in Germany until October 2011, when he was apprehended by German police. Pet. App. 3a, 12a; D. Ct. Doc. 27, at 5; D. Ct. Doc. 27-6, at 2, 4. German authorities ordered petitioner deported to the United States and banned him from entering Germany, or any other country within the Schengen Area, for five years, until 2016. Pet. App. 3a, 7a, 12a; D. Ct. Doc. 27, at 5-6; D. Ct. Doc. 27-3, at 2-3, 5.[1]

Following petitioner's return to the United States, he was convicted of escape in Colorado state court. D. Ct. Doc. 27, at 5. Petitioner's community corrections sentence was revoked, and he was sentenced to an additional year of imprisonment. *Ibid.*

b. In May 2015, although the five-year prohibition imposed in 2011 on his entering any Schengen Area

---

[1] The Schengen Area is "a group of European countries (not precisely coterminous with the European Union) where free travel across their various borders is permitted once a traveler is lawfully admitted to one of them." Pet. App. 12a n.1.

country was still in effect, petitioner nevertheless returned to Europe. Pet. App. 3a, 7a. He traveled from Denver to Iceland, where he was admitted to the Schengen Area, and traveled through the Netherlands, Belgium, and France—all Schengen Area countries—before arriving again in Germany, with plans to travel on to Morocco. See *id.* at 3a, 7a-8a, 11a-12a & n.1.

While in Germany, petitioner was again arrested, this time for violation of a German weapons law. Pet. App. 3a, 11a. After receiving a report that two men were target-shooting with guns in a field, German police investigated and found petitioner and another man in possession of multiple weapons, including a crossbow with a pistol grip and three gas-powered air rifles, possession of which violated German law. See D. Ct. Doc. 27, at 4; D. Ct. Doc. 27-1, at 2; D. Ct. Doc. 27-2, at 2-4. Petitioner was arrested, and upon learning that petitioner was in Germany in violation of the Schengen Area ban, German police interviewed him and questioned him about his travels. D. Ct. Doc. 27, at 4; D. Ct. Doc. 27-4, at 2-4. Petitioner described certain of his travels and stated that he wished to leave Germany and to travel to Morocco to be with his wife. D. Ct. Doc. 27, at 4; D. Ct. Doc. 27-1, at 3; D. Ct. Doc. 27-4, at 4; see Pet. App. 11a-12a. After holding petitioner overnight and completing identification procedures, German authorities determined that petitioner sought to leave Germany, and they released him and permitted him to depart for Morocco. D. Ct. Doc. 27, at 4-5; see D. Ct. Doc. 27-5.

German authorities subsequently informed the Federal Bureau of Investigation (FBI) of petitioner's arrest for weapons possession and that petitioner had entered Germany in violation of the Schengen Area ban imposed in 2011. Pet. App. 11a-12a; see D. Ct. Doc. 27, at 6. In

August 2015, the FBI relayed that information to Special Agent Kyle Allen of Homeland Security Investigations (HSI), a component of U.S. Immigrations and Customs Enforcement in the Department of Homeland Security (DHS). Pet. App. 11a; see D. Ct. Doc. 27, at 6. Special Agent Allen commenced an investigation and learned of petitioner's travel history, his address in Denver, and his criminal history, including prior felony convictions for trespass, fraud, use of a financial instrument, and escape. Pet. App. 13a. Special Agent Allen planned to interview petitioner if and when he returned to the United States. D. Ct. Doc. 27, at 6.

2. a. On November 13, 2015, terrorist cells operating in France and Belgium launched a large-scale attack on civilians in Paris. Pet. App. 3a, 13a. The terrorists, who were of Moroccan descent, "claimed allegiance to the Islamic [S]tate." *Id.* at 3a. Parts of France and Belgium "were 'on lockdown' for several days thereafter," and authorities were searching for suspects in those countries and Germany. *Id.* at 13a. Special Agent Allen reviewed his open case files and placed a "lookout" alert for petitioner in the United States Customs and Border Patrol (CBP) enforcement system. *Id.* at 3a-4a, 13a-14a.

On November 24, 2015, Special Agent Allen learned that petitioner had boarded a flight in Paris on a one-way ticket to Denver, with a layover in Iceland. Pet. App. 14a. Special Agent Allen went to the Denver airport in anticipation of petitioner's arrival. *Ibid.* He also arranged for two HSI computer forensic agents to be present in case petitioner was traveling with electronic devices. *Ibid.*

Upon arriving at the Denver airport, petitioner presented a signed standard customs declaration indicating his address in Denver. Pet. App. 14a. Petitioner's form

also stated that the only countries he had visited since leaving the United States were Belgium, France, and Morocco; he did not list Germany. *Ibid.* Special Agent Allen noticed that omission and determined that it was intentional, concluding that it was not "plausible" that petitioner had innocently forgotten his travel to Germany, where had been arrested and detained. 6/26/17 Tr. 42; see *id.* at 40-43; Pet. App. 14a-15a.

Special Agent Allen and Detective Craig Appel—a local police officer serving as a "deputized FBI 'task force officer'" on a "joint counterterrorism task force"—then interviewed petitioner for approximately 30 minutes. Pet. App. 15a. The agents asked petitioner about the purpose of his six-month trip abroad. *Id.* at 15a-16a. Petitioner claimed that he had traveled to Morocco to complete paperwork necessary to marry his then-fiancée, but that he had traveled back and forth between Morocco and Belgium because he was not allowed to remain in Morocco for more than six months at a time. *Id.* at 16a. Petitioner said that, for part of the time he spent in Belgium, he had stayed with a friend whom he met at a mosque, but he was unable to recall the friend's last name or the name of the mosque where they had met. *Ibid.* The agents also asked petitioner whether he had visited any countries other than those listed on his customs declaration—particularly Germany—but petitioner repeatedly gave evasive answers and did not admit having traveled to Germany. *Id.* at 4a, 17a-18a.

Meanwhile, other CBP agents searched petitioner's luggage and found a laptop and smartphone, which were password-protected. Pet. App. 15a. The HSI forensic agents were equipped with "light-weight forensic equipment" to attempt to bypass passwords, and if they were

able to unlock the devices, they planned to conduct a "triage review" of them. 6/26/17 Tr. 106-107. That process entails "quickly brows[ing] through the files and records immediately available on the device in question," rather than "a full forensic scan." Pet. App. 15a; see 6/26/17 Tr. 107 (triage review "is as brief as possible and on the surface" and focused on "quickly identifiable file types, such as images, documents; in the case of cell phones, text messages"). The agents attempted to unlock both devices but were unable to do so with the equipment they had at the airport. Pet. App. 15a.

Special Agent Allen and Detective Appel informed petitioner that the agents intended to search his laptop and smartphone and asked for the passwords. Pet. App. 4a, 16a. When petitioner declined to provide them, Special Agent Allen explained that his devices would be searched without his consent and would have to be taken to a different location and returned to him later. *Id.* at 5a, 16a-17a. Petitioner continued to refuse to provide his passwords and completed two claim forms for the return of the two devices. *Id.* at 17a. On each one, he listed an address in Denver different than the one he had provided on his customs declaration form (and previously on his passport application). *Ibid.* Petitioner was permitted to leave. *Id.* at 19a.

b. The following day, Special Agent Allen took petitioner's laptop and smartphone to an HSI office, where one of the HSI agents who had examined the devices at the airport and a colleague made a copy of the laptop's hard drive. Pet. App. 19a. Using more advanced software, one of the agents was able to bypass the laptop's password and generate a list of the hard drive's contents, including deleted folders. *Id.* at 20a. The agent neither inspected the previously lost or deleted data

that the software had recovered nor indexed the hard drive to enable searching. *Ibid.* Instead, he used the software only to view the contents "through a graphical user interface similar to what one would see if accessing the hard drive through the laptop" itself. *Ibid.*; see *id.* at 21a.

Within three minutes, the agent noticed a folder on the hard drive entitled "Issue 15 Little Duchess." Pet. App. 5a; see *id.* at 21a. The agent browsed that folder "as one could do if accessing it directly through the laptop" and discovered that it contained child pornography. *Id.* at 21a. The agent immediately ceased the search and notified Special Agent Allen, who then obtained a search warrant authorizing a complete forensic search of the hard drive. *Id.* at 5a. That search revealed thousands of images and videos of child pornography. *Ibid.*[2]

3. A grand jury in the United States District Court for the District of Colorado returned an indictment charging petitioner with one count of transporting child pornography, in violation of 18 U.S.C. 2252A(a)(1) and (b)(1), and one count of possessing child pornography, in violation of 18 U.S.C. 2252A(a)(5)(B) and (b)(2). Indictment 1-2.

Petitioner moved to suppress the evidence obtained from his laptop. See Pet. App. 10a. He contended that, while "routine searches of the persons and effects of entrants" at the border "are not subject to any requirement of reasonable suspicion, probable cause, or warrant," D. Ct. Doc. 19, at 8 (Mar. 27, 2017) (quoting *United States* v. *Montoya de Hernandez*, 473 U.S. 531, 538 (1985)), "more invasive," "non-routine" searches at

---

[2] Petitioner's smartphone was sent to a different lab for analysis, but no contraband files were found on it. Pet. App. 22a.

the border must be supported by "particularized, reasonable suspicion that the detained individual was currently, or imminently about to be, engaged in criminal activity," *id.* at 2, 7, 9, 12, 14; see *id.* at 12-14. Petitioner contended that, "[a]t the time [he] attempted to enter the United States at Denver International Airport, no evidence existed that would give rise to a reasonable suspicion that [he] was currently, or imminently about to be, engaged in criminal activity," and that the fruits of the warrantless search of his laptop should therefore be suppressed. *Id.* at 14; see *id.* at 14-15.

The district court denied the motion. Pet. App. 10a-38a. It noted that some courts have reasoned that, under the border-search exception to the warrant requirement, digital devices can be reasonably searched at the border without any suspicion, while other courts have distinguished between "manual" border searches of laptops and smartphones (for which they do not require suspicion) and "forensic" border searches (for which they require reasonable suspicion). *Id.* at 29a-30a. The district court, however, found it unnecessary to decide what level of suspicion, if any, would be required to conduct a manual or forensic search of an electronic device, or whether the search of petitioner's device was better characterized as "manual" or "forensic." *Id.* at 30a-31a.

The district court explained that, "[i]f reasonable suspicion existed (regardless of whether the Supreme Court would require it to exist), then under all of the authorities all parties have cited, the border search doctrine would permit the search that [was] conducted before [Special Agent] Allen obtained the search warrant." Pet. App. 31a. And the court determined that, on the facts of this case, "a reasonable official could suspect that [petitioner]

was attempting to conceal something about his travels abroad and also attempting to distance himself from his digital devices." *Id.* at 35a. The court accordingly held that a reasonable official could "conclude that [petitioner's] digital devices contained evidence of an ongoing crime, such as materials whose importation into or possession in the United States would be a violation of customs or other laws." *Ibid.*

Petitioner subsequently pleaded guilty to the indictment pursuant to a plea agreement. Judgment 1; Plea Agreement 1-17. In the plea agreement, petitioner stipulated that his laptop was found to contain more than 3500 images and 21 videos of child pornography—many of which were foreign-produced and depicted children as young as six years old. Plea Agreement 11-12. The district court accepted petitioner's plea and sentenced him to 84 months of imprisonment. Judgment 2.

4. The court of appeals affirmed. Pet. App. 1a-9a.

The court of appeals noted that petitioner had urged the court "to find that searches of personal electronic devices at the border must be supported by reasonable suspicion." Pet. App. 6a. But, like the district court, the court of appeals "decline[d] to do so," explaining that resolving that question was unnecessary in this case. *Ibid.* The court observed that, "under any interpretation of the Fourth Amendment put forth by [petitioner], reasonable suspicion is sufficient to justify a border search of personal electronic devices." *Ibid.* And because it "agree[d] with the district court that reasonable suspicion was present here," it determined that petitioner's "own arguments preclude[d] him from prevailing." *Ibid.*

The court of appeals found that "the totality of circumstances surrounding the search of [petitioner's] laptop readily meet[s] the reasonable suspicion standard," under

which "[l]aw enforcement officers must 'have an articulable, individualized, reasonable suspicion that an individual is involved in some criminal activity.'" Pet. App. 7a (quoting *United States* v. *Rascon-Ortiz*, 994 F.2d 749, 752 n.3 (10th Cir. 1993)). First, the agents knew that petitioner's "criminal history concerns border offenses": they knew that petitioner had fled the United States as a fugitive, and they "knew that [petitioner] had blatantly contravened" the ban that Germany had imposed on traveling to Germany or other Schengen Area countries. *Ibid.* Second, the agents knew that petitioner had been untruthful in recounting his travel history: they knew he had traveled to Germany but had "not list[ed] Germany as one of the countries visited on his customs declaration form despite attesting via signature that his answers on the form were truthful." *Ibid.* Third, the agents knew that petitioner "was returning to the United States on a one-way ticket originating in Paris—the site of devastating terrorist attacks less than two weeks earlier"; that his "travel itinerary included Belgium, France, and Morocco, three countries intimately linked to the attacks"; and that he had been arrested in Germany for "brandishing what appeared to be weapons." *Id.* at 8a. Finally, petitioner "appeared to distance himself from his electronic devices" when he provided a different address for their return than he had listed on his customs declaration form. *Ibid.*

The court of appeals noted petitioner's argument that reasonable suspicion of any criminal activity is insufficient and that, to conduct a forensic search of his laptop, an agent would need "reasonable suspicion that the search will turn up evidence that the person is inadmissible, carrying contraband, or evading customs duties." Pet. C.A. Br. 30. The court rejected that argument, observing that "[t]he Fourth Amendment does

not require [law enforcement] officers to close their eyes to suspicious circumstances." Pet. App. 8a-9a (quoting *Rascon-Ortiz*, 994 F.2d at 753) (brackets in original). And the court determined that "[t]he totality of the circumstances is sufficient to justify a warrantless search" of petitioner's laptop. *Id.* at 8a.

ARGUMENT

Petitioner contends (Pet. 31-34) that the warrantless search of his laptop by border agents upon his arrival at a port of entry violated the Fourth Amendment because the officers lacked reasonable suspicion that it contained digital contraband or reasonable suspicion of a crime related to the border-search exception's purposes. The court of appeals correctly upheld the border search, determining that, even assuming reasonable suspicion were required, the facts in this particular case established it. That case-specific determination does not warrant further review. And although the courts of appeals have articulated different approaches to the level and nature of the suspicion (if any) that is necessary to conduct a warrantless border search of an electronic device, this case does not implicate that disagreement, because the search of petitioner's laptop here was justified under any of the approaches petitioner urges. Further review is not warranted.

1. The "'border search' exception" is a "longstanding, historically recognized exception to the Fourth Amendment's general principle that a warrant be obtained" for a search. *United States* v. *Ramsey*, 431 U.S. 606, 621 (1977). That longstanding principle reflects that "[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). In addition, "the expectation of privacy [is] less at

the border than in the interior." *United States* v. *Montoya de Hernandez*, 473 U.S. 531, 539-540 (1985). Consequently, "the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is * * * struck much more favorably to the Government at the border." *Id.* at 540.

"Time and again, [this Court] ha[s] stated that 'searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border.'" *Flores-Montano*, 541 U.S. at 152-153 (quoting *Ramsey*, 431 U.S. at 616). The Court has explained that "[r]outine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant." *Montoya de Hernandez*, 473 U.S. at 538. And it has held, for example, that "the Government's authority to conduct suspicionless inspections at the border includes the authority to remove, disassemble, and reassemble a vehicle's fuel tank." *Flores-Montano*, 541 U.S. at 155.[3]

This Court has required a degree of individualized suspicion for a border search or seizure only once, in

---

[3] The border-search exception applies not only at international land borders but also at "international airport[s]" and other "'functional equivalent[s]'" of land borders. *United States* v. *Kolsuz*, 890 F.3d 133, 137 (4th Cir. 2018) (quoting *Almeida-Sanchez* v. *United States*, 413 U.S. 266, 272-273 (1973)). And the border-search exception applies here even though petitioner's devices were ultimately searched at a location other than the airport. "A border search of a computer is not transformed into an extended border search simply because the device is transported and examined beyond the border," *United States* v. *Cotterman*, 709 F.3d 952, 961 (9th Cir. 2013) (en banc), cert. denied, 571 U.S. 1156 (2014), and petitioner does not argue otherwise.

United States v. *Montoya de Hernandez*, *supra*. In that case, customs officers who reasonably suspected that a traveler was smuggling drugs in her alimentary canal detained her for 16 hours to monitor her bowel movements. 473 U.S. at 534-536. The Court upheld the seizure, explaining that "the detention of a traveler at the border, beyond the scope of a routine customs search and inspection, is justified at its inception if customs agents * * * reasonably suspect that the traveler is smuggling contraband in her alimentary canal." *Id.* at 541. The Court expressed "no view on what level of suspicion, if any, is required for nonroutine border searches such as strip, body-cavity, or involuntary x-ray searches." *Id.* at 541 n.4; cf. *Flores-Montano*, 541 U.S. at 152 (holding that lower court erred in extending *Montoya de Hernandez* to the factually dissimilar context of vehicle searches and observing that "[c]omplex balancing tests to determine what is a 'routine' search of a vehicle, as opposed to a more 'intrusive' search of a person, have no place in border searches of vehicles").

2. This Court has not specifically addressed the level of suspicion, if any, that is required for a search of an electronic device, such as a computer or smartphone, of a person arriving at the border. It is common ground that neither probable cause nor a warrant is necessary. "[N]o court has ever required a warrant for any border search or seizure." *United States* v. *Wanjiku*, 919 F.3d 472, 481 (7th Cir. 2019); accord, *e.g.*, *United States* v. *Kolsuz*, 890 F.3d 133, 147 (4th Cir. 2018); *United States* v. *Molina-Isidoro*, 884 F.3d 287, 292 (5th Cir. 2018). And petitioner did not contend below, and does not contend in this Court, that probable cause or a warrant is required for any border search of an electronic device.

Some lower courts have concluded that some form of reasonable suspicion is necessary to support what they have termed "forensic" searches of electronic devices. See, *e.g.*, *Kolsuz*, 890 F.3d at 144 ("[A] forensic border search of a phone must be treated as nonroutine, permissible only on a showing of individualized suspicion."); *United States* v. *Cotterman*, 709 F.3d 952, 968 (9th Cir. 2013) (en banc) (holding "that the forensic examination of [the defendant's] computer required a showing of reasonable suspicion"), cert. denied, 571 U.S. 1156 (2014); but cf. *United States* v. *Touset*, 890 F.3d 1227, 1229 (11th Cir. 2018) (concluding that "no suspicion is necessary to search electronic devices at the border"). Those courts have described such a "forensic" search as one that employs technology "capable of not only viewing data that a user has intentionally saved on a digital device, but also 'unlocking password-protected files, restoring deleted material, and retrieving images viewed on websites.'" *United States* v. *Aigbekaen*, 943 F.3d 713, 718 n.2 (4th Cir. 2019) (quoting *Cotterman*, 709 F.3d at 957). "[A]n integral part of a forensic examination is the use of technology-assisted search methodology, where the computer searches vast amounts of data that would exceed the capacity of a human reviewer to examine in any reasonable amount of time." *United States* v. *Saboonchi*, 990 F. Supp. 2d 536, 547 (D. Md. 2014). "The techniques used during a forensic search can be distinguished from a conventional [or manual] computer search, in which a Customs officer may operate or search an electronic device in much the same way that a typical user would use it." *Ibid.*

In the courts below and in this Court, petitioner has contended that a reasonable-suspicion standard should apply to a "forensic" search. Pet. i, 31; see D. Ct. Doc.

19, at 8-12; Pet. C.A. Br. 20-23. The court of appeals in this case, however, expressly reserved judgment on that issue. Pet. App. 6a. Like the district court, the court of appeals "decline[d]" to resolve whether "searches of personal electronic devices at the border must be supported by reasonable suspicion" because it determined, as had the district court, "that reasonable suspicion was present here." *Ibid.*; see *id.* at 30a-31a. That case-specific application of the reasonable-suspicion standard to the particular circumstances of this case was correct and does not warrant further review.

As the court of appeals found, "the totality of circumstances surrounding the search of [petitioner's] laptop readily meet[s] the reasonable suspicion standard." Pet. App. 7a. Before the limited search of petitioner's laptop was performed, agents knew of petitioner's significant "criminal history," which includes multiple felonies, and which "concerns border offenses." *Ibid.* Petitioner had previously fled this country as a fugitive and then "had blatantly contravened" an order excluding him from Germany and other Schengen Area countries. *Ibid.* Agents also knew that petitioner had lied about his travel abroad on his customs declarations form—omitting his travel to Germany, where he had been arrested for possessing unlawful weapons—"despite attesting via signature that his answers on the form were truthful." *Ibid.* Agents additionally knew that petitioner was returning from Paris, "the site of devastating terrorist attacks less than two weeks earlier," and that his travel also included other countries "intimately linked to the attacks." *Id.* at 8a. And they knew that petitioner "appeared to distance himself from his electronic devices" when confronted with the possibility that they would be retained by agents and returned at a later date. *Ibid.*

3. In this Court, petitioner does not appear to dispute the lower courts' factual findings or their application of reasonable-suspicion principles to those facts. See Pet. 31-34. And even if he did, any disagreement with the lower courts' factbound application of those principles to the circumstances of this case would not warrant plenary review. See Sup. Ct. R. 10; *United States* v. *Johnston*, 268 U.S. 220, 227 (1925) ("We do not grant a certiorari to review evidence and discuss specific facts."); see also *Kyles* v. *Whitley*, 514 U.S. 419, 456-457 (1995) (Scalia, J., dissenting) ("[U]nder what we have called the 'two-court rule,' the policy [in *Johnston*] has been applied with particular rigor when district court and court of appeals are in agreement as to what conclusion the record requires." (citing *Graver Tank & Mfg. Co.* v. *Linde Air Prods. Co.*, 336 U.S. 271, 275 (1949))).

Petitioner instead contends (Pet. 32-34) that a forensic border search of an electronic device must be supported by a more specific form of reasonable suspicion—namely, "reasonable suspicion of digital contraband or of evidence of a crime related to the border search exception's purposes," Pet. 33—and that the court of appeals erred by upholding the search without finding that the facts supported a reasonable suspicion of that kind. That contention does not warrant review.

a. As a threshold matter, it is unclear that the court of appeals understood petitioner to be advancing the specific reasonable-suspicion standard he now proposes. It instead appears to have perceived his then-proposed standard to be significantly narrower.

In the district court, petitioner had not urged a border-specific version of the reasonable-suspicion standard. To the contrary, he argued that the district court should

apply ordinary reasonable-suspicion principles to "forensic search[es]" of electronic devices at the border and should hold that such a search "must be supported by particularized, reasonable suspicion that the detained individual was currently, or imminently about to be, engaged in criminal activity." D. Ct. Doc. 19, at 14; see *id.* at 12-14.

Petitioner observed that this Court "has defined reasonable suspicion as a particularized and objective basis for suspecting the particular person stopped of criminal activity," D. Ct. Doc. 19, at 12 (citing *United States* v. *Cortez*, 449 U.S. 411, 417-418 (1981)), and that "[t]his standard is met when law enforcement can point to specific and articulable facts and rational inferences that can be drawn from those facts indicating that criminal activity may be afoot," *id.* at 12-13 (citing *Terry* v. *Ohio*, 392 U.S. 1 (1968)) (emphasis omitted). He asserted that "the reasonable suspicion standard relates to ongoing or imminent criminal activity, not historic acts." *Id.* at 13. And he contended that the search here was unjustified because there was no "specific, articulable fact or set of facts that would support a conclusion that there was reasonable suspicion that [petitioner] was engaged, or about to be engaged, in criminal activity when he was stopped at customs." *Id.* at 13. The district court rejected petitioner's contention on its own terms, Pet. App. 30a-35a; petitioner did not make, and the court did not address, an argument that only reasonable suspicion of contraband or of crimes linked to the border-search exception's purposes can justify a forensic search of electronic devices at the border.

In the court of appeals, petitioner took a different tack. He contended that "the forensic search of [his]

laptop could be valid only if the agents reasonably suspected" a "violation of one of the Government's border interests," which petitioner specifically defined as suspicion "that [petitioner] wasn't entitled to enter the country, that he was carrying contraband, or that he was evading customs duties." Pet. C.A. Br. 27; accord Pet. C.A. Reply Br. 19-23. In response, the government explained that petitioner's proposed conception of the "concerns underlying the border-search exception" was too narrow and disregarded customs officials' principal role as "law enforcement agents," whose "statutory responsibilities * * * include 'detecting, responding to, and interdicting terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other persons who may undermine the security of the United States.'" Gov't C.A. Br. 42-43 (quoting 6 U.S.C. 211(c)(5)) (brackets omitted).

The court of appeals appears, like the government, to have understood petitioner to be advocating a crabbed contraband-or-customs-laws-only version of the reasonable-suspicion inquiry. Pet. App. 8a (petitioner "suggest[ed] that border agents are tasked exclusively with upholding customs laws and rooting out the importation of contraband" and that, "because border agents did not suspect him of either of these types of crimes, they were prevented from searching his laptop and cell phone"). The court rejected petitioner's argument thus framed. *Ibid.* The court did not directly pass upon the soundness of the intermediate standard petitioner now advocates (Pet. 33)—which requires "reasonable suspicion of digital contraband or of evidence of a crime related to the border search exception's purposes" more generally—or on the application of such a standard to this case.

b. In any event, petitioner's contention that the court of appeals should have applied a narrower, border-specific version of the reasonable-suspicion inquiry does not warrant review in this case. Application of petitioner's proposed standard would not alter the result the court reached, for two reasons.

First, like the lower-court decisions on which he relies, petitioner does not contend that every border search of an electronic device requires reasonable suspicion. He acknowledges (Pet. 1) that "travelers may expect routine searches without any suspicion." Accord Pet. 4 (recognizing that "routine searches" at the border "require neither a warrant nor suspicion of criminal activity"). Petitioner urges, and lower courts have applied, a reasonable-suspicion standard only to those particularly comprehensive or invasive searches that courts have labeled "forensic." *E.g.*, Pet. i, 31, 33; see Pet. 12-21 (discussing lower-court cases); see also, *e.g.*, *Kolsuz*, 890 F.3d at 144; *Cotterman*, 709 F.3d at 967-968.

As the government explained in the court of appeals, the search of petitioner's laptop resembles routine, manual searches, as to which lower courts do not require suspicion, much more closely than the type of forensic analysis described above, see p. 14, *supra*, as to which some lower courts have required reasonable suspicion. Gov't C.A. Br. 27-32. After bypassing petitioner's password protection—the software equivalent of using a tool to open a locked briefcase that a traveler refuses to unlock for inspection—the agent who performed the search simply skimmed through a list of active folders on the laptop for less than three minutes. Although the agent used external software to bypass the password and copy the data, the agent did not view any lost or deleted files,

create any special search algorithms, or access petitioner's electronic communications or search history. See Pet. App. 5a, 19a-21a; see pp. 6-7, *supra*.

The district court and the court of appeals declined to reach the question whether that search was forensic because they each determined that the search was supported by reasonable suspicion in any event. Pet. App. 5a, 31a. The district court did observe, however, that the agent browsed the folders on petitioner's laptop "as one could do if accessing it directly from the laptop." *Id.* at 21a. And several other courts have recognized that software-assisted searches of electronic devices qualify as manual (rather than forensic) searches where, as here, the program was used to circumvent user passwords but the duration of the search was relatively short and it accessed information that would also be accessible to a manual user examining the electronic devices. See, *e.g.*, *United States* v. *Lopez*, No. 13-cr-2092, 2016 WL 7370030, at *4 (S.D. Cal. Dec. 20, 2016); *United States* v. *Smasal*, No. 15-cr-85, 2015 WL 4622246, *4, *8 (D. Minn. June 19, 2015).

Petitioner could not prevail on his own theory unless he demonstrated, and a court found, that the initial, brief search the agents conducted constituted the type of "forensic" examination that he contends triggers a reasonable-suspicion requirement. If the search was more akin to a routine, manual search, then even he has not contended that suspicion was necessary. Neither court below decided how to categorize this particular search, and petitioner identifies no sound reason for this Court to decide that antecedent, factbound question in the first instance.

Second, even assuming that the search of petitioner's laptop could be justified only with reasonable suspicion

of criminal offenses linked to the concerns underlying the border-search exception, the facts of this case would satisfy that requirement. See Gov't C.A. Br. 42-46. The facts that the court of appeals identified that supported reasonable suspicion of criminal activity were facts that more specifically pointed to potential offenses implicating those concerns. As the court observed, petitioner's "criminal history concern[ed] border offenses," and he had just been arrested again in Germany after violating the five-year travel prohibition and traveling undetected through several Schengen Area countries. Pet. App. 7a. Upon arriving in this country, petitioner proceeded to provide a materially false statement on his customs form concerning that recent international travel, *ibid.*—itself an offense, see generally 18 U.S.C. 1001.

And in light of the deception on petitioner's customs form, the agents could reasonably suspect that he was engaged in unlawful activity that would interfere with the "collection of [customs] duties." *Montoya de Hernandez*, 473 U.S. at 537. Indeed, the fact that petitioner "appeared to distance himself from his electronic devices," Pet. App. 8a, by stating that his devices should be returned to a different address than the one that he had listed for himself, suggested that the devices he was attempting to bring into the country were suspect. As the district court concluded, "[a] reasonable official could * * * conclude that [petitioner's] digital devices contained evidence of an ongoing crime, such as materials whose importation into or possession in the United States would be a violation of customs or other laws." *Id.* at 35a.

Furthermore, the additional facts the court of appeals recited—that petitioner "was returning to the

United States on a one-way ticket originating in Paris" where "devastating terrorist attacks" had just occurred; that his "travel itinerary included Belgium, France, and Morocco, three countries intimately linked to the attacks"; that he "gave vague answers regarding his time in Belgium"; and that he "had been arrested in Germany for brandishing what appeared to be weapons," Pet. App. 4a, 8a—all gave the agents cause for concern that petitioner posed a threat to "national security." *Aigbekaen*, 943 F.3d at 721. Taken together, the agents had reasonable suspicion of multiple offenses bearing a nexus to the border-search exception's purposes. Although the court of appeals did not specifically apply petitioner's proposed test, the facts that it and the district court found weigh decisively against petitioner even if that test applies.

c. Although petitioner principally argues that reasonable suspicion of the presence of contraband "*or* of evidence of a crime related to the border search exception's purposes" suffices to authorize a forensic search, Pet. 33 (emphasis added); see also Pet. 31, he briefly asserts (Pet. 33) in passing that "the border search exception authorizes warrantless searches of the digital data on electronic devices only on reasonable suspicion that it contains contraband." To the extent that he is in fact urging that even more cramped view of border-search authority, that contention does not warrant review.

Petitioner did not properly preserve an argument below that only reasonable suspicion of contraband suffices. He did not advance that argument in the district court or in his appellate briefs. He advocated it only cursorily in a post-briefing letter under Federal Rule of Appellate Procedure 28(j) apprising the panel of the Ninth Circuit's decision in *United States* v. *Cano*, 934 F.3d

1002 (2019), petition for reh'g pending, No. 17-50151 (filed Jan. 2, 2020), which adopted that approach, see *id.* at 1020 ("[T]o conduct a more intrusive, forensic cell phone search border officials must reasonably suspect that the cell phone to be searched itself contains contraband."); see Pet. C.A. Rule 28(j) Ltr. 2 (Aug. 16, 2019).[4] But in keeping with its own practice of not addressing issues not raised in a party's briefing, including arguments made for the first time in a Rule 28(j) letter, see *United States* v. *Kimler*, 335 F.3d 1132, 1138 n.6 (10th Cir.), cert. denied, 540 U.S. 1083 (2003), the Tenth Circuit did not address that unpreserved contraband-only argument in this case. This Court's "traditional rule * * * precludes a grant of certiorari * * * when 'the question presented was not pressed or passed upon below.'" *United States* v. *Williams*, 504 U.S. 36, 41 (1992) (citation omitted).

In any event, petitioner's passing contention lacks merit. Petitioner asserts that "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.'" Pet. 32 (quoting *Boyd* v. *United States*, 116 U.S. 616, 623 (1886)) (brackets in

---

[4] The Ninth Circuit additionally concluded that, while "[m]anual searches of a cell phone at the border can be conducted without any suspicion whatsoever," border agents conducting such manual searches "are limited to searching for contraband only," and "may not search in a manner untethered to the search for contraband." *Cano*, 934 F.3d at 1019. Petitioner's Rule 28(j) letter did not discuss this separate conclusion. See Pet. C.A. Rule 28(j) Ltr. 1-2. The Ninth Circuit's opinion in *Cano* did not address other recognized reasons for the border-search exception, such as helping to determine the admissibility of travelers and national-security concerns.

original). But this Court later rejected that distinction in *Warden* v. *Hayden*, 387 U.S. 294 (1967), which held that "there is no viable reason to distinguish intrusions to secure 'mere evidence' from intrusions to secure fruits, instrumentalities, or contraband." *Id.* at 310; see *United States* v. *Gurr*, 471 F.3d 144, 149 (D.C. Cir. 2006) (citing *Hayden* for the proposition that "[t]he distinction * * * between contraband and documentary evidence of a crime is without legal basis"), cert. denied, 550 U.S. 919 (2007). Any limitation of the border-search exception to searches for contraband itself is therefore inconsistent with this Court's precedent.

Moreover, as discussed above, see p. 19, *supra*, petitioner acknowledges (Pet. 1, 4) that any requirement of individualized suspicion applies at most only to forensic searches and not routine, manual searches. The contraband-only reasonable-suspicion test petitioner urges thus would not benefit him unless he first demonstrates that the search in this case was forensic in that sense.

4. Petitioner additionally contends (Pet. 12-26) that this Court's review is warranted to resolve inconsistency in the approaches several courts of appeals have taken in evaluating searches of electronic devices at the border. Although lower courts have articulated differing approaches, this case does not implicate any circuit disagreement.

The Eleventh Circuit has determined that "no suspicion is necessary to search electronic devices at the border," even "for forensic searches of electronic devices at the border." *Touset*, 890 F.3d at 1229, 1231; see *id.* at 1229-1234. The Eleventh Circuit in that case found, in the alternative, that if reasonable suspicion were required for the search in that case, it existed. See *id.* at

1237-1238. The Fourth and Ninth Circuits have concluded that reasonable suspicion is required for "forensic," but not manual, searches of such devices. The Fourth Circuit has stated that, to conduct an "intrusive, nonroutine forensic" search of a digital device "under the border search exception (that is, without a warrant), the Government must have individualized suspicion of an offense that bears some nexus to the border search exceptions' 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 Ninth Circuit has stated that, "to conduct a more intrusive, forensic cell phone search border officials must reasonably suspect that the cell phone to be searched itself contains contraband." *Cano*, 934 F.3d at 1020. Neither court, however, requires a showing of reasonable suspicion for manual, non-"forensic" searches. See *id.* at 1007-1008; *Cotterman*, 709 F.3d at 960-967; *United States* v. *Ickes*, 393 F.3d 501, 503 (4th Cir. 2005).

The petition here does not implicate the tension among those approaches. The Tenth Circuit expressly reserved judgment on whether reasonable suspicion is required for the type of search conducted in this case. Instead, it found that the facts supported reasonable suspicion in any event. Pet. App. 8a.

As petitioner acknowledges (Pet. 22-26), the search in this case would be upheld under the Eleventh Circuit's approach. Petitioner suggests (Pet. 12, 18-21, 26) that the Fourth Circuit would not sustain the search because the lower courts did not specifically identify facts supporting reasonable suspicion of an offense linked to the border-search exception's purposes. As explained above, however,

it is far from clear that the search here is the sort of "forensic" search to which the Fourth Circuit's approach is limited, see *Aigbekaen*, 943 F.3d at 721, and in any event the facts of this case did support reasonable suspicion of offenses that implicate the concerns underlying the border-search exception. See pp. 19-22, *supra*.

Petitioner also suggests (Pet. 12-17, 26) that the Tenth Circuit's approach here is inconsistent with the Ninth Circuit's decisions in *Cotterman* and particularly *Cano*, in which that court stated that a forensic search requires reasonable suspicion that the device to be searched contains digital contraband. See 934 F.3d at 1014-1017, 1020. The panel's decision in *Cano* is inconsistent with the standards articulated and applied by other courts. But it does not warrant further review in this case. As noted above, petitioner did not properly preserve an argument that only reasonable suspicion of the presence of contraband suffices, and the court of appeals did not address that argument. See pp. 22-23, *supra*. Furthermore, to the extent that petitioner would rely on the Ninth Circuit's requirement of reasonable suspicion of contraband as a prerequisite for "forensic" searches, he has not shown, and neither court below found, that the search in this case qualifies. See pp. 19-20, *supra*.[5]

---

[5] In addition, as noted above, p. 23 n.4, *supra*, the Ninth Circuit panel in *Cano* did not address other established reasons for the border-search exception, including national-security concerns. As also noted above, see *ibid.*, the Ninth Circuit in *Cano* limited the scope of suspicionless manual searches to portions of the device on which contraband could be found. See 934 F.3d at 1007, 1013-1014, 1019-1020. But petitioner has not argued that, if the search here was manual, it was unconstitutional. In any event, it is far from clear that the brief review of the list of files on petitioner's laptop exceeded the boundaries of a permissible manual search as described in *Cano*. See *id.* at 1019.

In addition, the government has filed a petition for rehearing en banc of the Ninth Circuit's decision in *Cano*. See Pet. for Reh'g at 1-3, 6-18, *Cano*, *supra* (No. 17-50151). That petition and a response called for by the court of appeals are currently pending. If rehearing is granted, the en banc court's decision may eliminate any disagreement between the *Cano* panel's holding and the approaches of other circuits. Granting review in this posture to address inconsistency with the Ninth Circuit's outlier position would therefore be premature. Further review is not warranted.

CONCLUSION

The petition for a writ of certiorari should be denied.

Respectfully submitted.

NOEL J. FRANCISCO
Solicitor General
BRIAN A. BENCZKOWSKI
Assistant Attorney General
DANIEL N. LERMAN
Attorney

JUNE 2020