No. 13-186

In the Supreme Court of the United States

HOWARD WESLEY COTTERMAN, PETITIONER

v.

UNITED STATES OF AMERICA

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

BRIEF FOR THE UNITED STATES IN OPPOSITION

DONALD B. VERRILLI, JR.
Solicitor General
Counsel of Record
MYTHILI RAMAN
Acting Assistant Attorney General
ROSS B. GOLDMAN
Attorney
Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217

QUESTIONS PRESENTED

1. Whether the court of appeals committed reversible error in deciding whether the border search of petitioner's computer was justified based on reasonable suspicion, when the government initially argued that no individualized suspicion was required, the court of appeals requested supplemental briefing on whether reasonable suspicion was present, and the government argued that if reasonable suspicion were required, such reasonable suspicion was present here.

2. Whether the search of petitioner's computer was supported by reasonable suspicion.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases:

Cases—Continued: Page

Statutes:

Statutes—Continued: Page

In the Supreme Court of the United States

No. 13-186

HOWARD WESLEY COTTERMAN, PETITIONER

v.

UNITED STATES OF AMERICA

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

BRIEF FOR THE UNITED STATES IN OPPOSITION

OPINIONS BELOW

The opinion of the en banc court of appeals (Pet. App. 1-85) is reported at 709 F.3d 952. A prior opinion of the court of appeals is reported at 637 F.3d 1068. The order of the district court (Pet. App. 86-88) is unreported but is available at 2009 WL 465028.

JURISDICTION

The judgment of the en banc court of appeals was entered on March 8, 2013. On June 4, 2013, Justice Kennedy extended the time within which to file a petition for a writ of certiorari to and including July 6, 2013. On June 20, 2013, Justice Kennedy further extended the time to August 5, 2013, and the petition was filed on that date. The jurisdiction of this Court is invoked under 28 U.S.C. 1254(1).

STATEMENT

A grand jury in the United States District Court for the District of Arizona returned an indictment charging petitioner with production of child pornography, in violation of 18 U.S.C 2251(a) and (e); transportation and shipping of child pornography, in violation of 18 U.S.C. 2252(a)(1) and (b)(1); receipt of child pornography, in violation of 18 U.S.C. 2252(a)(2) and (b)(1); possession of child pornography, in violation of 18 U.S.C. 2252(a)(4)(B) and (b)(2); importation of obscene materials, in violation of 18 U.S.C. 1462(a); transportation of obscene materials, in violation of 18 U.S.C. 1465; and flight to avoid prosecution, in violation of 18 U.S.C. 1073. The district court granted petitioner's motion to suppress evidence of child pornography found during a forensic search of his laptop computer. Pet. App. 86-88. A panel of the court of appeals reversed the suppression holding. *United States* v. *Cotterman*, 637 F.3d 1068 (9th Cir. 2011). The en banc court of appeals also reversed the suppression holding. Pet. App. 1-85.

1. On April 6, 2007, petitioner and his wife were returning to the United States from Mexico through the Lukeville, Arizona, port of entry. Pet. App. 5. During primary inspection at the border checkpoint, a government computer system (the TECS database[1]) returned a hit for petitioner, informing U.S. Customs and Border Protection (CBP) officers that he was a

[1] The TECS database is a Department of Homeland Security database that includes information about individuals suspected of criminal activity. Pet. App. 5 n.3.

convicted sex offender[2] and was suspected of child sex tourism. *Id.* at 5-6.

Based on this information, petitioner and his wife were referred for secondary inspection. Pet. App. 6. CBP officers followed up on the TECS alert by calling the contact person associated with petitioner's entry in the database; from that call, the officers learned that petitioner was suspected of involvement in child pornography. *Ibid.* CBP officers searched petitioner's vehicle and found two laptop computers and three digital cameras. *Ibid.* A CBP officer turned on one of the laptop computers and saw several password-protected files. *Ibid.*; Gov't C.A. Br. 6.

CBP officers contacted the U.S. Immigration and Customs Enforcement (ICE) office in Sells, Arizona. Pet. App. 6. They reported that petitioner was a convicted sex offender suspected of child sex tourism who was seeking to enter the United States, and that he had a computer with several password-protected files. *Id.* at 6-7. The ICE duty agent contacted the office responsible for the TECS alert to learn more about petitioner's suspected criminal activity. *Id.* at 6. She learned that the alert was part of Operation Angel Watch, a law enforcement operation aimed at fighting child sex tourism by identifying registered sex offenders in California who frequently travel outside the United States. *Ibid.* Based on that information, the ICE duty agent determined that it would be appropriate to conduct a forensic examination of petitioner's computers. *Id.* at 7.

---

[2] In 1992, petitioner was convicted on two counts of using a minor in sexual conduct, two counts of lewd and lascivious conduct upon a child, and three counts of child molestation. Pet. App. 5-6.

The ICE duty agent and a supervisor traveled from Sells to the Lukeville port of entry to speak with petitioner and his wife. Pet. App. 7. The agents gave petitioner *Miranda* warnings and then interviewed him. *Ibid.* During the interview, petitioner offered to help the agents access the password-protected files on his computer, but the agents declined, fearing that petitioner might delete the files or that the laptop might be "booby trapped." *Ibid.* The agents allowed petitioner and his wife to depart the border but detained the two laptop computers and one of the digital cameras. *Ibid.*

An ICE agent then took the computers and camera to the ICE office in Tucson, Arizona, for further examination. Pet. App. 7. That night and the next day, a forensic examiner searched the computers using special software and found that one of the computers contained 75 images of child pornography. *Id.* at 7-8, 91.[3] The examiner contacted petitioner and asked him to come in to help access password-protected files. *Id.* at 8. Petitioner agreed to come in, but then he fled to Sydney, Australia. *Ibid.* Two days later, the forensic examiner managed to open the password-protected files and found 378 images of child pornography. *Ibid.* Many of the images featured petitioner sexually molesting a girl between the ages of 7 and 10. *Ibid.* Over the next few months, the forensic examiner found hundreds more pornographic images and videos depicting children. *Ibid.*

---

[3] The examiner found no contraband on the camera or on petitioner's wife's computer, and so he returned those items. Pet. App. 7, 91.

In September 2007, petitioner was arrested by Australian law enforcement officers and was extradited back to Arizona. Gov't C.A. Br. 11.

2. A grand jury in the United States District Court for the District of Arizona returned an indictment charging petitioner with two counts of production of child pornography, in violation of 18 U.S.C 2251(a) and (e); one count of transportation and shipping of child pornography, in violation of 18 U.S.C. 2252(a)(1) and (b)(1); one count of receipt of child pornography, in violation of 18 U.S.C. 2252(a)(2) and (b)(1); one count of possession of child pornography, in violation of 18 U.S.C. 2252(a)(4)(B) and (b)(2); one count of importation of obscene materials, in violation of 18 U.S.C. 1462(a); one count of transportation of obscene materials, in violation of 18 U.S.C. 1465; and one count of flight to avoid prosecution, in violation of 18 U.S.C. 1073. Indictment 1-5 (07-CR-01207 Docket entry No. 9) (D. Ariz. June 27, 2007).

Petitioner moved to suppress the evidence obtained from the search of his computer, contending that the search of his computer was a "non-routine" border search that required at least reasonable suspicion. See Mot. to Suppress 4-11 (07-CR-01207 Docket entry No. 17) (D. Ariz. Apr. 18, 2008); see Pet. App. 92. In response, the government argued that no individualized suspicion was required for the forensic examination of petitioner's computer. Sealed Resp. to Def. Mot. to Suppress 9-13 (07-CR-01207 Docket entry No. 31) (D. Ariz. July 9, 2008).

The magistrate judge recommended that the suppression motion be granted. Pet. App. 89-109. In the magistrate judge's view, because the search occurred away from the border and took several days to com-

plete, the search was an extended border search and reasonable suspicion was required. *Id.* at 96-99. The magistrate judge then concluded that the officers lacked reasonable suspicion here. *Id.* at 99-105.

The government objected to the magistrate judge's report and recommendation on two grounds: first, no individualized suspicion was required for the computer search, and second, in any event, the search here was supported by reasonable suspicion. See Gov't Objections to Magistrate's Report & Recommendation 6-25 (07-CR-01207 Docket entry 60) (D. Ariz. Sept. 26, 2008). In response, petitioner contended that the magistrate judge correctly concluded that reasonable suspicion was required to search the computer and reasonable suspicion was lacking here. See Reply to Gov't Objections 3-9 (07-CR-01207 Docket entry 62) (D. Ariz. Oct. 3, 2008).

In a brief order, the district court adopted the magistrate judge's report and recommendation and suppressed the evidence obtained from the search of petitioner's computer. Pet. App. 86-88.

The government appealed the suppression holding, arguing that the forensic search of petitioner's laptop for child pornography does not require individualized suspicion. Pet. App. 9.

3. The court of appeals reversed. See *United States* v. *Cotterman*, 637 F.3d 1068 (9th Cir. 2011). The court held that no individualized suspicion was required for the search of petitioner's laptop computer because it was a routine border search. *Id.* at 1070, 1079. The court rejected petitioner's argument that the search of his computer no longer qualified as a border search because the computer was taken to a facility away from the border, explaining that "the

inherent power of the Government to subject incoming travelers to inspection before entry also permits the Government to transport property not yet cleared for entry away from the border to complete its search." *Id.* at 1076. A contrary rule, the court explained, would "reward those individuals who, either because of the nature of their contraband or the sophistication of their criminal enterprise, hide their contraband more cleverly" and would give those individuals an incentive "to seek entry at more vulnerable points less equipped to discover them." *Id.* at 1078. The court then reviewed the particular facts of this case and concluded that it was reasonable for the officers to take the computers offsite to search them and that the government used "reasonable diligence and speed in conducting the computer forensic examination," finding the child pornography within 48 hours. *Id.* at 1080-1083.

Judge Betty Fletcher dissented, taking the view that officers could not search and seize the computer without reasonable suspicion that the computer contained evidence of a particular crime. *Cotterman*, 637 F.3d at 1086.

4. The court of appeals granted rehearing en banc. Following oral argument, the court ordered supplemental briefing on two questions: (1) whether the court could reverse the district court's suppression order by reversing its finding that no reasonable suspicion existed to search petitioner's laptop computer, even though the government did not appeal that finding, and (2) whether the district court's finding of no reasonable suspicion was supported by the record. Order 1-2 (09-10139 Docket entry No. 85) (9th Cir. June 29, 2012); Order 1-2 (09-10139 Docket entry No.

83) (9th Cir. June 26, 2012); see also Pet. App. 9-10. Both parties filed supplemental briefs addressing these questions. As relevant here, the government argued that the court had the authority to reach the reasonable suspicion question and that the officers had reasonable suspicion under the circumstances here. Gov't Supp. C.A. Br. 2-10 (09-10139 Docket entry No. 86) (9th Cir. July 20, 2012).

The en banc court of appeals reversed the suppression order. Pet. App. 1-85. The court first concluded that it had the authority to address whether the computer search was justified based on reasonable suspicion even though the government did not make that argument in its initial appellate briefs. *Id.* at 10-11. The court explained that the dispute before it "necessarily encompasses a determination as to the applicable standard"—"no suspicion, reasonable suspicion or probable cause"—and that consideration of whether reasonable suspicion justifies the search will not prejudice petitioner because the court called for supplemental briefs and petitioner was able to provide his argument on that issue. *Ibid.* (citing, *inter alia*, *United States* v. *Resendiz-Ponce*, 549 U.S. 102, 103-104 (2007)).

The court then concluded that, although the government generally does not need individualized suspicion to search items at the border, reasonable suspicion was required for the forensic analysis of petitioner's computer. Pet. App. 11-27. The court recognized 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 11 (quoting *United States* v. *Flores-Montano*, 541 U.S. 149, 152 (2004) (brackets in original)), and that "border searches are

generally deemed 'reasonable simply by virtue of the fact that they occur at the border,'" *ibid.* (quoting *United States* v. *Ramsey*, 431 U.S. 606, 616 (1977)). But the court concluded that reasonable suspicion was required for the search of petitioner's computer because of the "comprehensive and intrusive nature of a forensic examination." *Id.* at 16-17. The court did not attempt to "define[] the precise dimensions of a reasonable border search," instead calling for a "case-by-case analysis." *Id.* at 17.

Finally, the court of appeals concluded that reasonable suspicion supported the computer search in this case. Pet. App. 28-34. The court explained that such suspicion existed based on the totality of the circumstances, which included the alert in the TECS database as part of Operation Angel Watch, petitioner's prior convictions for child sex offenses, petitioner's frequent international travels, petitioner's entry from a country known for sex tourism, petitioner's collection of electronic equipment, and the fact that several files on petitioner's computer were password-protected. *Id.* at 29-32. The court rejected the view that this reasonable suspicion was dispelled by petitioner's offer to help access the files and the agents' failure to find any incriminating material when they first turned on the computer, explaining that "[c]ollectors of child pornography can hardly be expected to clearly label such files and leave them in readily visible and accessible sections of a computer's hard drive." *Id.* at 32-33. The court explained that once the officers encountered password-protected files, that fact, combined with the TECS alert and the facts noted above, "justified obtaining additional resources,

here available in Tucson, to properly determine whether illegal files were present." *Id.* at 33.

Judge Callahan, joined by Judge Clifton and joined in part by Judge Milan Smith, concurred in part, dissented in part, and concurred in the judgment. Pet. App. 34-55. Judge Callahan agreed that the officers had reasonable suspicion in this case, *id.* at 35, but would have held that no individualized suspicion is required for a forensic examination of a computer at the border, *id.* at 38-50.

Judge Milan Smith dissented. Pet. App. 55-85. Writing for himself and Judges Clifton and Callahan, Judge Smith explained that individualized suspicion generally is not required at the border. *Id.* at 59-71. Writing only for himself, Judge Smith would have held, however, that reasonable suspicion was required for this computer search because it did not occur at the border, *id.* at 73-76, and that the officers lacked reasonable suspicion here, *id.* at 76-84. Judge Smith also would have held that the court should not have reached the existence of reasonable suspicion because the government had initially not raised it. *Id.* at 71-73.

ARGUMENT

Petitioner contends (Pet. 10-37) that certiorari is warranted because, in his view, the court of appeals erred in considering whether reasonable suspicion justifies the search of his computer and in concluding that reasonable suspicion was present here. The court of appeals acted within its discretion in deciding the reasonable suspicion question, and its factbound holding does not conflict with any decision of this Court or of any other court of appeals. Further review is therefore unwarranted.

1. Petitioner first contends (Pet. 16-17, 25-33) that the court of appeals erred by resolving the case on reasonable suspicion grounds when the government did not challenge the district court's reasonable suspicion holding in its initial appellate briefs. He is mistaken.

a. It is well established that courts of appeals have discretion to order supplemental briefing on issues not previously raised and to resolve cases based on those issues. As this Court has explained, "[w]hen an issue or claim is properly before the court, the court is not limited to the particular legal theories advanced by the parties, but rather retains the independent power to identify and apply the proper construction of governing law." *United States Nat'l Bank* v. *Independent Ins. Agents of Am.*, 508 U.S. 439, 446 (1993) (citation omitted; brackets in original). In *United States National Bank*, respondents did not challenge the validity of the statute at issue (12 U.S.C. 92) before the district court or the court of appeals, and when the court of appeals requested supplemental briefing on the issue after oral argument, they "urge[d] the court to resolve the issue, while still taking no position on the merits." 508 U.S. at 444-445. The court of appeals nonetheless considered the issue and decided it in respondents' favor. *Id.* at 444. This Court held both that the court of appeals had the power to consider the issue and that it acted prudently in doing so. *Id.* at 446-448. The Court explained that a "case or controversy" existed before the court of appeals, and that court "may consider an issue 'antecedent to . . . and ultimately dispositive of' the dispute before it, even an issue the parties fail to identify and brief." *Id.* at 446-447 (citation omitted).

Based on those principles, the court of appeals acted within its discretion in addressing the reasonable suspicion issue in this case. The court considered that issue bound up in the question whether the computer search in this case was permissible, and it gave the parties an opportunity for supplemental briefing to ensure that the issue was fully aired. Pet. App. 10-11; see *United States Nat'l Bank*, 508 U.S. at 448 (noting that court of appeals "g[ave] the parties ample opportunity to address the issue" through post-argument supplemental briefing). In this case, as in *United States National Bank*, "the Court of Appeals did not stray beyond its constitutional or prudential boundaries." *Id.* at 447.

Contrary to petitioner's contention (Pet. 29-30), the court of appeals' consideration of the reasonable suspicion issue did not unfairly prejudice him. The issue had been raised and briefed in the district court. Although the government took the position that no individualized suspicion was required for the search of petitioner's computer, it argued in the alternative that reasonable suspicion was present. See Gov't Objections to Magistrate's Report & Recommendation 20-25 (07-CR-01207 Docket entry 60) (D. Ariz. Sept. 26, 2008). Petitioner responded to that argument before the district court. See Reply to Gov't Objections 7-9 (07-CR-01207 Docket entry 62) (D. Ariz. Oct. 3, 2008); see also Pet. 5. On appeal, the government did not raise the issue to the panel (before which it prevailed), but when the en banc court of appeals issued its supplementary briefing order, petitioner had the opportunity to argue the reasonable suspicion issue before the appellate court ruled on it. Where, as here, the parties are afforded the opportunity to file supple-

mental briefs on an issue, a reviewing court may properly resolve a case on that ground, even if the ground was raised for the first time in the supplemental briefs. See Pet. App. 10-11; see also, *e.g.*, *Trest* v. *Cain*, 522 U.S. 87, 92 (1997) ("We do not say that a court must always ask for further briefing when it disposes of a case on a basis not previously argued. But often, as here, that somewhat longer (and often fairer) way 'round is the shortest way home."); *United States* v. *Nadler*, 698 F.2d 995, 998 (9th Cir. 1983) (court permissibly decided issue raised for first time in supplemental briefing).

Petitioner contends (Pet. 29-30) that had the government challenged the adverse reasonable suspicion holding in its opening brief, his answering brief would have argued that reasonable suspicion was lacking. But petitioner presented that very argument through supplemental briefs. See Resp. to Gov't Supp. Br. 14-20 (09-10139 Docket entry 91) (9th Cir. Aug. 20, 2012). Petitioner's opportunity to brief the reasonable suspicion issue before the court of appeals ruled on it likewise defeats any potential due process claim (Pet. 32-33), because petitioner had an "opportunity to be heard." *Mathews* v. *Eldridge*, 424 U.S. 319, 333 (1976). Petitioner cannot claim prejudice on the ground that he ultimately lost on the reasonable suspicion issue, see Pet. 30, because prejudice in this context is based on procedural fairness, not substantive outcomes. See, *e.g.*, *Alcaraz* v. *INS*, 384 F.3d 1150, 1161 (9th Cir. 2004). The court of appeals' rejection of petitioner's argument does not constitute cognizable prejudice once he had the opportunity to be heard.

b. Contrary to petitioner's contention (Pet. 16-17), the circuits do not disagree about whether a court of appeals may address an issue presented for the first time in supplemental briefs. The cases petitioner cites (Pet. 17 n.5) state the general proposition that arguments not raised in an appellant's opening brief are abandoned and not subject to appellate review. The government does not dispute that, under court rules and practice, appellate courts may appropriately decline to pass on issues not raised in the appellant's opening brief. But the cases cited by petitioner do not hold that a court lacks the authority, in the exercise of its discretion, to request supplemental briefing on an otherwise unpreserved argument and to decide a case based on those grounds. To the contrary, although generally "courts of appeals do not decide questions which were not raised properly in the parties' briefs," they nonetheless "have the discretionary authority to raise and consider" such questions. *B & G Constr. Co.* v. *Director, Office of Workers' Comp. Programs*, 662 F.3d 233, 246 n.15 (3d Cir. 2011).

This Court and the courts of appeals have repeatedly acknowledged their authority to consider issues not initially raised or preserved by the parties. See, *e.g.*, *United States* v. *Resendiz-Ponce*, 549 U.S. 102, 103-104 (2007) (after oral argument, Court ordered parties to submit supplemental briefs on an issue not raised by the government and then resolved the case in favor of the government on that ground); *United States* v. *Ingram*, 594 F.3d 972, 979 n.3 (8th Cir.) ("[T]his court has raised issues *sua sponte* on behalf of criminal defendants where a plain error affected substantial rights, * * * and we have never said that the authority to do so runs only one way in a criminal

case."), cert. denied, 131 S. Ct. 222 (2010); *Mitchell* v. *Fishbein*, 377 F.3d 157, 164-165 (2d Cir. 2004) ("This Court has ample discretion to excuse an appellant's failure to argue an issue in his opening brief and to give the parties a further opportunity to address the issue."); *United States* v. *Southern Fabricating Co.*, 764 F.2d 780, 781 (11th Cir. 1985) ("The decision whether to consider * * * an argument [raised for the first time on appeal] is left to the appellate court's discretion."); *United States* v. *Brown*, 555 F.2d 407, 420 n.29 (5th Cir. 1977) (court requested supplemental briefs before ruling on grounds not originally raised by appellants), cert. denied, 435 U.S. 904 (1978). Accordingly, no further review is warranted on the first question presented.

2. Petitioner contends (Pet. 33-37) that the court of appeals erred in concluding that the forensic search of his computer was supported by reasonable suspicion. The court of appeals' factbound conclusion is correct, does not conflict with a decision of any other court of appeals, and does not warrant further review by this Court.

a. Reasonable suspicion is a suspicion of criminal activity based on "specific and articulable facts which, taken together with rational inferences from those facts," give rise to the inference that crime is afoot. *Terry* v. *Ohio*, 392 U.S. 1, 21 (1968). "To satisfy this standard, more than a mere 'hunch' of wrongdoing is required, but 'considerably' less suspicion is needed than would be required to 'satisf[y] a preponderance of the evidence standard.'" *Safford Unified Sch. Dist. No. 1* v. *Redding*, 557 U.S. 364, 384 (2009) (quoting *United States* v. *Arvizu*, 534 U.S. 266, 274 (2002)). Whether reasonable suspicion exists depends on the

totality of the circumstances, *id.* at 385, and facts that may seem innocent may, when combined with other facts, establish a reasonable suspicion of criminal activity, see *United States* v. *Sokolow*, 490 U.S. 1, 9-10 (1989). See also, *e.g.*, *Terry*, 392 U.S. at 22 (Court considered "a series of acts, each of them perhaps innocent" if viewed separately, "but which taken together warranted further investigation").

The court of appeals correctly concluded that the totality of the facts in this case gave rise to a reasonable suspicion of criminal activity. The TECS database alert indicated that petitioner was suspected of child sex tourism. Pet. App. 5-6, 28-29. A CBP officer and an ICE agent followed up on that alert and learned that petitioner was suspected of being involved in child pornography as part of Operation Angel Watch, which targeted registered sex offenders who frequently traveled internationally. *Id.* at 6, 29-30. They also learned that petitioner had three prior convictions for child sex offenses. *Id.* at 5-6, 28-29; see note 2, *supra*. Petitioner was returning from a country associated with sex tourism. *Id.* at 29-30; see, *e.g.*, *United States* v. *Irving*, 452 F.3d 110, 114 (2d Cir. 2006); *United States* v. *Julian*, 427 F.3d 471, 475 (7th Cir. 2005), cert. denied, 546 U.S. 1220 (2006). When an officer turned on petitioner's laptop computer, he saw several password-protected files; although those files could have had an innocent explanation, they also suggested that petitioner may have been protecting contraband. Pet. App. 30-32. Although no evidence of that contraband was found when officers first turned on the computer, that did not dispel the suspicion, because "making illegal files difficult to access makes perfect sense for a suspected holder of child pornography." *Id.* at

31-33. When considered as a whole, these facts clearly established "more than an inchoate and unparticularized suspicion or hunch," *United States* v. *Montoya de Hernandez*, 473 U.S. 531, 542 (1985), and the court of appeals therefore correctly found reasonable suspicion here.

b. Petitioner suggests (Pet. 4, 6) that the officers who conducted the computer search did not rely on reasonable suspicion to conduct their search. That is immaterial: whether reasonable suspicion exists depends on objective consideration of the facts available to the officers, and the officers' subjective beliefs do not matter. See, *e.g.*, *Ohio* v. *Robinette*, 519 U.S. 33, 38-39 (1996). In any event, petitioner is wrong to suggest (Pet. 13, 35) that the CBP officers and ICE agents involved in the search of petitioner's laptop computer believed they lacked reasonable suspicion to support a search. The record excerpts petitioner cites do not support that view; rather, they are the officers' testimony that they did not find anything incriminating during the initial search of petitioner's computer. See C.A. Supp. R.E. 87, 98-99, 164, 173. And, more to the point, one CBP officer testified that he believed the TECS alert indicated that petitioner was involved "in some type of child pornography." Pet. App. 6 (quoting officer's testimony at evidentiary hearing).

Petitioner also contends (Pet. 33-34) that the court of appeals used the wrong legal standard in evaluating reasonable suspicion, citing this Court's decision in *United States* v. *Arvizu*, *supra*. But the court of appeals used the same legal standard as in *Arvizu*: whether, under the totality of the circumstances, the objective and articulable facts observed by officers supported a reasonable suspicion of criminal activity.

Compare Pet. App. 28-33 (asking whether there is a "particularized and objective basis for suspecting the particular person stopped of criminal activity" under "the totality of the circumstances"), with *Arvizu*, 534 U.S. at 273 (explaining that in making "reasonable-suspicion determinations" reviewing courts "must look at the totality of the circumstances of each case to see whether the detaining officer has a particularized and objective basis for suspecting legal wrongdoing") (internal quotation marks omitted).[4]

Petitioner is wrong to suggest that the court of appeals "cherry-pick[ed] which factors to consider" (Pet. 34); the court considered "factors weighing both in favor and against reasonable suspicion," and it concluded that petitioner's offer to access his computer and the officers' failure to find any incriminating material immediately upon accessing the computer did not dispel the reasonable suspicion that existed by reason of the TECS database alert, petitioner's prior child sex convictions, petitioner's frequent interna-

---

[4] Petitioner contends (Pet. 19) that the court of appeals' holding that forensic examinations of computers at the border require reasonable suspicion conflicts with the Fifth Circuit's decision in *United States* v. *Roberts*, 274 F.3d 1007 (2001). In *Roberts*, a border-search case involving an outbound traveler, the Fifth Circuit held that law enforcement's forensic examination of the defendant's computer discs was justified based on the defendant's consent or, in the alternative, because the defendant's admission that the discs contained images of child pornography provided probable cause. *Id.* at 1016-1017. The court did not discuss what level of suspicion would be necessary for such a search, likely because the presence of both consent and probable cause made such an analysis unnecessary. See *id.* at 1012 (stating that "constitutional issues should be decided on the most narrow, limited basis" available).

tional travel, his return from a country known for child sex tourism, and the password-protected files on his laptop. Pet. App. 32-33. As this Court noted in *Arvizu*, the possibility of an innocent explanation for some of the facts does not undermine the presence of reasonable suspicion. 534 U.S. at 274-275. Petitioner's argument ultimately is a factbound disagreement with the conclusion of the court below, and such a disagreement does not warrant this Court's review.

3. Petitioner makes a variety of other arguments, none of which warrants this Court's review. First, petitioner contends (Pet. 10, 11) that this is a "watershed case" about the scope of the government's search authority at the border. But petitioner does not contend that the court of appeals adopted the wrong legal standard for the search of his computer. Petitioner argued to the court of appeals that reasonable suspicion was required to justify the search of his computer, Pet. C.A. Br. 18-48, and the court of appeals agreed with that argument and held that reasonable suspicion was required for this particular search, Pet. App. 24-27. In his petition, petitioner does not quarrel with that legal standard, but simply takes issue with the court of appeals' application of that familiar reasonable-suspicion standard to the facts of his case.

The government has argued throughout this litigation and still contends that no individualized suspicion was required to justify the search of petitioner's computer in this case. The government's search authority is "at its zenith at the international border," *United States* v. *Flores-Montano*, 541 U.S. 149, 152-153 (2004), and that authority is not dissipated because "some property presented for entry—and not yet admitted or released from the sovereign's control—

[must] be transported to a secondary site for adequate inspection," *United States* v. *Cotterman*, 637 F.3d 1068, 1070, aff'd, 709 F.3d 952 (9th Cir. 2013) (en banc). Accordingly, the judgment below could be affirmed on that basis. See, *e.g.*, *Washington* v. *Confederated Bands & Tribes of Yakima Indian Nation*, 439 U.S. 463, 476 n.20 (1979). Nonetheless, the court of appeals agreed with petitioner that reasonable suspicion is required under these circumstances and petitioner challenges only whether the court of appeals properly applied that test here.

Petitioner next contends (Pet. 12-16) that the court of appeals erred in holding that border officers may "seize any item or items they wish, take them anywhere, and hold them for days, even weeks or months, all without any reasonable suspicion that any criminality is occurring." That statement does not accurately reflect the court of appeals' holding. The court specifically rejected the notion that "anything goes" in a border search, Pet. App. 11, explaining that "[t]he reasonableness of a search or seizure depends on the totality of the circumstances, including the scope and duration of the deprivation," *id.* at 12. The court upheld the particular forensic search in this case, which occurred approximately 170 miles from the border, started immediately after the computer was brought to the ICE office, and lasted 48 hours before the officers found contraband. *Id.* at 6-7; *id.* at 40-41, 48 (Callahan, J., concurring in part, dissenting in part, and concurring in the judgment). The court did not address other searches, stating that they should await "case-by-case analysis." *Id.* at 17.

Petitioner also contends (Pet. 12-13) that suppression is required not because the forensic examination

of the computer is an illegal search, but "because the search resulted from an unreasonable *seizure*." But the court of appeals appropriately considered whether the detention of the computer and the forensic search were justified as one question, because the reason that the officers detained the computer was to conduct a forensic examination of its contents. See Pet. App. 11-34. The detention of petitioner's computer in order to search it was justified by the same reasons that justified the search of the computer itself.[5] Moreover, this was not an "unreasonably prolonged * * * seizure" (Pet. 14); approximately 48 hours passed from the time the agents retained the laptop computer in Lukeville to the time the forensic examiner discovered 75 images of child pornography on the computer. Pet. App. 5-8; see also *Cotterman*, 637 F.3d at 1083 (government used "reasonable diligence and speed in conducting the computer forensic examination"). Although petitioner now seeks to distinguish between the search and the seizure, the court of appeals did not consider that argument, and this Court should not address it in the first instance.

Finally, petitioner contends (Pet. 17-21) that review is warranted to determine the precise contours of the "extended border search" doctrine adopted by various courts of appeals. But the court of appeals did

---

[5] Petitioner suggests in passing (Pet. 15) that "while property may be detained for a suspicionless search upon crossing the border, outright seizure and removal demands * * * probable cause followed by a warrant." But this is not a case of "outright seizure and removal," because petitioner's laptop computer never cleared customs, and it was only moved away from the border in order to access the particular tools required to conduct an adequate search. See *Cotterman*, 637 F.3d at 1081-1082.

not rely on any "extended border search doctrine." The court of appeals explained that the "key feature of an extended border search is that an individual can be assumed to have cleared the border and thus regained an expectation of privacy in accompanying belongings," and that did not occur here. Pet. App. 13. No reason exists to address any differences in the circuits' articulation of an "extended border search doctrine," because it would not affect the outcome in this case. Petitioner contends (Pet. 17-21) that the court of appeals should have treated the forensic search in this case as an extended border search requiring reasonable suspicion.[6] But the court of appeals did require reasonable suspicion, so whether the search here is termed an "extended border search" or not, the result in this case would be the same. For this reason as well, further review is unwarranted.

CONCLUSION

The petition for a writ of certiorari should be denied.

Respectfully submitted.

DONALD B. VERRILLI, JR.
Solicitor General
MYTHILI RAMAN
Acting Assistant Attorney General
ROSS B. GOLDMAN
Attorney

NOVEMBER 2013

[6] Each of the cases cited by petitioner applied the reasonable suspicion standard to extended border searches. See *United States* v. *Yang*, 286 F.3d 940, 947-949 (7th Cir. 2002); *United States* v. *Espinoza-Seanez*, 862 F.2d 526, 530-532 (5th Cir. 1988); *United States* v. *Bilir*, 592 F.2d 735, 740-741 (4th Cir. 1979).