No. 20-1043

IN THE
SUPREME COURT OF THE UNITED STATES

United States of America,

Petitioner,

v.

Miguel Angel Cano,

Respondent.

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

BRIEF IN OPPOSITION

Jeffrey L. Fisher
STANFORD LAW SCHOOL
SUPREME COURT LITIGATION
CLINIC
559 Nathan Abbott Way
Stanford, CA 94305

Harini P. Raghupathi
Counsel of Record
FEDERAL DEFENDERS
OF SAN DIEGO, INC.
225 Broadway, Suite 900
San Diego, CA 92101
(619) 234-8467
Harini_Raghupathi@fd.org

QUESTION PRESENTED

Whether extensive searches of respondent Miguel Angel Cano's cell phone incident to his arrest at the border—without a warrant or any individualized suspicion that the phone contained contraband—violated the Fourth Amendment.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Constitutional Provisions

Statutes

Legislative Materials

Other Authorities

INTRODUCTION

In this case, the Ninth Circuit held that neither a warrant nor individualized suspicion is required to conduct manual searches of certain types of content on cell phones seized incident to arrest at the border. The court of appeals concluded that the particular searches at issue here nevertheless violated the Fourth Amendment because they exceeded the permissible scope of a border search. Specifically, it held that border searches may be conducted only to prevent contraband from entering the country, whereas the agents here searched the contents of respondent Miguel Angel Cano's phone even after it was apparent that it contained no digital contraband.

The Government asks this Court to grant certiorari to review the Ninth Circuit's holding on the permissible scope of a border search. The Court should deny that request. The Ninth Circuit's reasoning is sound, and there is at most one court of appeals, the First Circuit, whose precedent might now require it to decide this case differently. Moreover, the practical import of any divergence between these two circuits could well be minimal.

Resolving the narrow question the Government frames would also require the Court simultaneously to address whether a warrant—or at least some level of individualized suspicion of contraband—is required to search digital devices incident to an arrest at the border. The Court denied certiorari earlier this Term in a case raising that issue, *see United States v. Williams*, 942 F.3d 1187 (10th Cir. 2019), *cert. denied*, 141 S. Ct. 235 (2020), and the issue still has not percolated sufficiently in the lower courts. Among other things, the lower courts have yet to

fully consider how this Court's relatively recent decision in *Riley v. California*, 573 U.S. 373 (2014), positive law dating back to the Founding, the expressive nature of the digital content at issue, and the Government's retention policies may affect the constitutional analysis. Additionally, technological developments may soon transform the relevant terrain, and legislative action may obviate any need for this Court to address the issue at all.

Meanwhile, waiting for these evolving dynamics to play out will not threaten any pressing governmental interest or disrupt the daily work of border officials. The Government regularly seeks warrants to search cell phones incident to arrest at the border. And when obtaining a warrant is not feasible, several legal doctrines other than the border-search exception may enable agents to search phones. At any rate, *this* case is certainly not one where agents had any need to dispense with seeking a warrant before searching Mr. Cano's phone for evidence of border-related crime. If a future scenario arises in which the Government can truly claim that it needs to conduct a warrantless search of a cell phone at the border for such evidence, the Court could then consider whether to extend the border-search exception in the manner the Government requests here. At this moment, the Court's intervention would be premature.

STATEMENT OF THE CASE

A. Factual background

1. Respondent Miguel Angel Cano is a lawful permanent resident of the United States. For over twenty years, he lived with his wife and two children outside of Los Angeles, where he worked with his father and brother in the carpet

and flooring-installation trade. In June 2016, the family business experienced a downturn, leaving Mr. Cano with just two full days of work per week. In July, he temporarily relocated to Tijuana, Mexico, where he could stay with his cousin for free and look for work in nearby San Diego.

2. Later that month, Mr. Cano planned another of his regular border crossings from Tijuana. As usual, he was carrying his smartphone. He arrived early in the morning at the San Ysidro Port of Entry and underwent the standard primary inspection. C.A. E.R. 16. He was then randomly selected for a secondary inspection. During that inspection, a narcotics-detecting dog alerted agents to a spare tire mounted on the exterior of his truck. Pet. App. 3a. At 6:45 AM, CBP officers took Mr. Cano into custody, placing him in ankle cuffs inside a nearby security office and removing all items on his person. C.A. E.R. 4, 16-17. CBP agents then ran the truck through an x-ray machine, which revealed anomalies in the spare tire. An agent removed the tire and cut it open, finding cocaine. At 8:00 AM, CBP officers formally arrested Mr. Cano and summoned Homeland Security Investigations (HSI), a unit that investigates drug-smuggling cases. *Id.* 16-17.

About one hour later, HSI Agents Petonak and Medrano arrived. C.A. E.R. 17. At that point, customs agents had possessed Mr. Cano's phone for over two hours. Agent Petonak picked up Mr. Cano's phone and manually scrolled through its digital contents, including the call log, text messages, and third-party messaging apps WhatsApp and Facebook Messenger. *Id.* 188-89. Agent Petonak later testified that he was trying to "find some brief investigative leads in the current case" and to

"see if there [was] evidence of other things coming across the border." Pet. App. 4a (internal quotation marks omitted).

After another hour, Agent Medrano conducted a second manual search of the phone, which was continuing to receive incoming messages. He again examined the call log, text message folder, and third-party messaging apps. Pet. App. 4a-5a; C.A. E.R. 123-24. He wrote down the phone numbers associated with some of Mr. Cano's incoming, missed, and outgoing calls. C.A. E.R. 123. He also noted two WhatsApp messages from Mr. Cano's cousin: one received at 6:24 AM, just as Mr. Cano was arriving at the border ("Good morning"), and another received at 12:03 PM, hours after the phone had been seized ("Primo are you coming to the house?"). *Id.* 123, 1064. Agent Medrano took a picture of the WhatsApp screen showing both messages. Pet. 6.

Agent Medrano also conducted a "logical download" search of Mr. Cano's phone using Cellebrite software. Pet. App. 5a. Such a download extracts the digital contents of apps holding text messages, contacts, call logs, multimedia messages (i.e., photos and videos), calendar events, notes, task lists, and "application data" from a cell phone. C.A. E.R. 410, 1027. The results of the download can then be viewed and saved in government databases for later inspections.

3. Two weeks later, with Mr. Cano still in custody, the Government sought and received a search warrant for the phone. Pet. 6. The resulting search did not produce any new, pertinent evidence. *Id.*

B. Procedural history

1. The Government charged Mr. Cano with conspiracy to import and importation of cocaine into the United States. Pet. 6-7. Before trial, it dropped the conspiracy charge. Following a trial on the remaining charge, the jury could not reach a verdict, and the district court declared a mistrial. *Id.* 7.

On retrial, Mr. Cano maintained (as he had in the first trial) that, on the day in question, he intended to look for work at a carpet store in the San Diego area. C.A. E.R. 808-09. Mr. Cano explained that his cousin must have placed the drugs in the spare tire of his truck without his knowledge. Pet. App. 6a-8a. Mr. Cano further explained that his cousin was a longtime member of a gang known to smuggle drugs across the border. *Id.* 36a-37a. The cousin also had access to the truck and had borrowed it shortly before Mr. Cano attempted to cross the border. C.A. E.R. 812-13.

To fend off this defense, the Government presented evidence procured from the three post-arrest, warrantless searches of Mr. Cano's cell phone. Specifically, the Government introduced the empty text message log, the call log, and the two WhatsApp messages, including one that Mr. Cano received after his phone had already been seized. Pet. 7. The Government also argued in closing that Mr. Cano deleted his text messages before crossing the border because he wanted to hide any drug-related communications from the agents. C.A. E.R. 946-47. Mr. Cano had objected that this evidence should be excluded because the searches of his cell phone violated the Fourth Amendment. But the district court overruled that objection.

The jury found Mr. Cano guilty, and the district court sentenced him to fifty-four months of imprisonment. Pet. 2.

2. The Ninth Circuit reversed and remanded. As relevant here, it held that "most" of the evidence the Government introduced at trial from Mr. Cano's cell phone had been procured in violation of the Fourth Amendment. Pet App. 33a.

As an initial matter, the Ninth Circuit adhered to its previous holding in *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013) (en banc), *cert. denied*, 571 U.S. 1156 (2014), that federal agents need not procure warrants to search cell phones at the border. Pet App. 17a-20a. Rebuffing the contention that this Court's intervening decision in *Riley v. California*, 573 U.S. 373 (2014), required reconsideration of *Cotterman*, the court of appeals reaffirmed *Cotterman*'s holdings that "manual searches of cell phones at the border are reasonable without individualized suspicion, whereas the forensic examination of a cell phone requires a showing of reasonable suspicion." Pet. App. 19a-20a.

The court of appeals then turned to whether the searches here "exceeded the proper scope of a border search." Pet. App. 21a. Stressing that the border-search exception is rooted in the right of the sovereign to enforce customs laws and interdict contraband, *id.* 13a-15a (citing *Carroll v. United States*, 267 U.S. 132, 154 (1925), and *United States v. Ramsey*, 431 U.S. 606, 620 (1977)), the court of appeals held that the exception "authorizes warrantless searches of a cell phone only to determine whether the phone contains contraband," *id.* 26a.

Applying that limitation on the permissible scope of border searches, the court of appeals held that the agents' initial manual search of the text messages app on Mr. Cano's phone—in which they discovered that he had deleted all of his text messages before arriving at the port of entry—was permissible because at least one

form of contraband (child pornography) "may be sent via text message." Pet. App. 27a. The court of appeals also condoned the agents' initial inspection of the phone's call log "to verify that the log contained a list of phone numbers" and not any digital contraband. *Id.* But the agents' continued search of the phone, during which they recorded "phone numbers and [the WhatsApp] messages" received after Mr. Cano's arrival at the port of entry, violated the Fourth Amendment because by that point it was clear "that the phone lacked digital contraband." *Id.* 27a-28a.

The court of appeals further held that "if the Cellebrite search of Cano's cell phone qualifies as a forensic search, the entire search was unreasonable under the Fourth Amendment." Pet. App. 30a. That was so, the court of appeals reasoned, because the "reasonable suspicion" test in the context of border searches requires reasonable suspicion *of contraband*, and the agents did not "reasonably suspect that the cell phone . . . itself contain[ed] contraband." *Id.* "In cases such as this," the Ninth Circuit stated, "where the individual suspected of committing the border-related crime has already been arrested, there is no reason why border officials cannot obtain a warrant before conducting their forensic search." *Id.* The court of appeals, however, "decline[d] to reach" whether "the Cellebrite search constitute[d] a forensic search," sending the issue back for the district court to address in the first instance. *Id.* 30a n.12, 33a-34a.

Finally, the court of appeals held that the good-faith exception to the exclusionary rule did not apply here. The strand of that exception relating to prior judicial precedent applies "only when the officials have relied on '*binding* appellate precedent.'" Pet. App. 33a (citation omitted). The HSI agents here "could not rely on

Cotterman to justify a search for *evidence*; *Cotterman* was a search for *contraband* that the government has a right to seize at the border." *Id.* 32a.

3. The Ninth Circuit denied the Government's petition for rehearing en banc. Pet. App. 61a.

REASONS FOR DENYING THE WRIT

I. Any conflict regarding the constitutionality of the searches here is shallow and nascent.

Assessing whether a search of a cell phone at the border comports with the Fourth Amendment depends on two sub-inquiries. First, did the agent have the requisite level of suspicion (if any) to conduct the search? Second, if so, did the scope of the agent's search exceed constitutional limitations? The requisite level of suspicion for border searches of cell phones may inform the permissible scope, and vice versa. For example, any particularized suspicion requirement will imply a certain permissible scope in accordance with that suspicion; a warrant requirement will result in even more explicit directives about what places on a phone can be searched and for what information. On the other hand, if no suspicion is required (at least in particular circumstances) to search cell phones, that may create a greater need to constrain the scope of such searches. In short, to determine whether a cell phone search at the border comports with the Fourth Amendment, it is necessary to consider both the requisite level of suspicion and the proper scope.

None of the courts of appeals the Government references in its petition has resolved both of those sub-issues in a manner that would dictate a different outcome here. After the Government filed its petition, the First Circuit issued an opinion

indicating it might have held the searches here comported with the Fourth Amendment. *Alasaad v. Mayorkas*, 988 F.3d 8 (1st Cir. 2021), *petition for cert. filed sub nom. Merchant v. Mayorkas* (No. 20-1505). But that holding arose in a very different context and creates at most a nascent disagreement with uncertain practical import.

1. Contrary to the Government's suggestions, there is no conflict between the Ninth Circuit and the Fourth or Tenth Circuits concerning whether the searches conducted here violated the Fourth Amendment.

In *United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018), the Fourth Circuit rejected a defendant's argument that evidence seized during a border search of his cell phone should have been suppressed, ultimately holding that the good-faith exception to the exclusionary rule permitted introduction of the evidence. *Id.* at 137. The Government notes that the Fourth Circuit ruled that border searches of digital devices need not be limited to inspections for contraband. *See* Pet. 9-10. But the Fourth Circuit did "not resolve" the overarching question whether the search in that case violated the Fourth Amendment. *Kolsuz*, 890 F.3d at 147. Instead, the Fourth Circuit reserved the question whether heightened suspicion or even a warrant might be required for *any* search of a digital device (manual or forensic) at the border. *Id.* at 137, 141 ("What precisely that standard should be—whether reasonable suspicion is enough, as the district court concluded, or whether there must be a warrant based on probable cause . . . is a question we need not resolve."). Accordingly, it is unclear whether the Fourth Circuit would have held that the warrantless searches at issue here comported with the Fourth Amendment.

In *United States v. Williams*, 942 F.3d 1187 (10th Cir. 2019), *cert. denied*, 141 S. Ct. 235 (2020), a border agent searched the electronic devices of a traveler suspected of having connections to terrorist attacks. The Tenth Circuit deemed the search constitutional. As the Government notes, the Tenth Circuit rejected the argument that "border agents are tasked exclusively with upholding customs laws and rooting out the importation of contraband." Pet. 24 (quoting *Williams*, 942 F.3d at 1191). But the key word there is "exclusively." As the Government itself stressed when opposing certiorari in that case, the Tenth Circuit found the fact that the defendant "posed a threat to 'national security'" independently justified the border search. *Williams* BIO at 22 (No. 19-1221) (citation omitted).

No national-security concerns were present here, and the Government "does not construe [the Ninth Circuit's decision below] to foreclose reliance" on "national-security" grounds to "sustain border searches of cell phones in appropriate circumstances." Pet. 19 n.*. Thus, the Tenth Circuit's decision does not conflict with the decision below.

2. The Government also claims the Ninth Circuit's decision is in "tension" with decisions from the Fifth and Seventh Circuits. Pet. 24. But both of those cases were resolved under the good-faith exception. Neither adopted a Fourth Amendment rule that would have required the courts to hold that the searches here were constitutional. *See United States v. Molina-Isidoro*, 884 F.3d 287, 290 (5th Cir. 2018) ("We do not decide the Fourth Amendment question."); *United States v. Wanjiku*, 919 F.3d 472, 479 (7th Cir. 2019) ("[W]e need not adopt either of these

positions, and indeed may avoid entirely the thorny issue of the appropriate level of suspicion required . . . because these agents acted in good faith.").

3. Nor do the two other cases the Government cites conflict with the decision below. The Eleventh Circuit held in *United States v. Touset*, 890 F.3d 1227 (11th Cir. 2018), that a border search of digital devices comported with the Fourth Amendment where agents "had a particularized and objective basis for suspecting that [the defendant] possessed child pornography on his electronic devices." *Id.* at 1237 (citation and internal quotation marks omitted). And the D.C. Circuit in *United States v. Gurr*, 471 F.3d 144, 147 (D.C. Cir. 2006), *cert. denied*, 550 U.S. 919 (2007), did not consider digital devices at all, but rather a search of "luggage." The Ninth Circuit would have decided *Touset* the same way, and there is no reason to think the cell-phone-specific rule below would restrict border searches of physical items like the luggage in *Gurr*.

4. The First Circuit's recent decision in *Alasaad* does appear to diverge from the Ninth Circuit's decision in this case. *Alasaad* (now called *Merchant* in this Court) is a civil case in which plaintiffs seek to enjoin the Government from enforcing its policies governing searches of electronic devices at the border. The plaintiffs allege that border agents have searched their electronic devices in the past and that they fear such searches in the future. *Alasaad v. Nielsen*, 419 F. Supp. 3d 142, 151-53 (D. Mass. 2019). They maintain, as relevant here, that the Fourth Amendment requires a warrant, or at least reasonable suspicion of

contraband, to search digital devices at the border.[1] The First Circuit rejected both arguments.

The First Circuit also stated that it disagreed with the Ninth Circuit's holding in this case that border searches of digital devices must be limited in scope to inspections for contraband. *Alasaad*, 988 F.3d at 20-21. Yet none of the plaintiffs in that case was arrested or alleges a fear of being arrested at the border in the future. The First Circuit thus had no occasion to determine whether the additional fact of an arrest at the border would mean that a warrant (or at least individualized suspicion of contraband) should be required before searching a cell phone. So it is not certain whether the First Circuit's facially categorical holdings would apply to searches of cell phones seized incident to an arrest at the border. Conversely, it is not clear the Ninth Circuit would apply the constitutional limitation it announced here to a case, like *Merchant*, that did not involve an arrest. The Ninth Circuit stressed, for example, that, "*in cases such as this*, where the individual suspected of committing the border-related crime has already been arrested, there is no reason why border officials cannot obtain a warrant before conducting their forensic search." Pet. App. 30a (emphasis added). Absent future decisions confronting those questions on concrete facts, the extent of any disagreement between the courts remains uncertain.

---

[1] The Government challenged the plaintiffs' standing in the district court, arguing that their "risk of future injury is too speculative" to support their Fourth Amendment claims. *Alasaad*, 419 F. Supp. 3d at 150. The district court rejected that argument. *Id.* at 150-53. The Government did not renew the contention in the First Circuit, and the First Circuit did not consider the issue for itself. 988 F.3d at 15 n.5.

II. Further percolation is warranted.

Insofar as the First and Ninth Circuits truly disagree, this recent fissure between two circuits does not call for this Court's immediate review.

A. More time is necessary to understand the practical import of any divergence between the Ninth and First Circuits.

It is too early to say whether the Ninth Circuit's rule limiting border searches of cell phones to inspections for digital contraband meaningfully limits the scope of searches compared to the First Circuit's view of the Fourth Amendment, or whether it will produce the same search authority and results.

For one thing, the Government suggests that digital contraband may be "a category limited almost exclusively to child pornography." Pet. 26. But that is not so. Contraband is typically defined to include any goods that are "unlawful to import, export, produce, or possess." *Contraband*, *Black's Law Dictionary* (11th ed. 2019). Accordingly, as the Government has stated elsewhere, there appear to be "many types of 'digital contraband,'" including "classified information, stolen credit card numbers, counterfeit media, and programs designed specifically to hack into other computers." *See* Def.'s Mem. Supp. Summ. J. at 13, *Alasaad v. Duke*, No. 1:17-cv-11730 (D. Mass. June 6, 2019) (ECF No. 97). In fact, several courts have recently confronted border-search cases involving these types of data and treated them as digital contraband. *See, e.g.*, *United States v. Qin*, 2020 WL 7024650, at *8 (D. Mass. 2020) (recognizing "the export of technical data for controlled exports," including "proprietary data, trade secrets, schematics diagrams, [and] technical know-how," as "digital contraband"); *Gowadia v. United States*, 2015 WL 5838471,

at *5 (D. Haw. 2015) (indicating that e-mails containing NASA codes and B-2 and F-5E bomber designs can violate the Arms Export Control Act).

More important, it remains to be seen which apps on a phone are subject to searches for contraband. If the contraband rule allows limited searches of most or all phone apps, the Ninth Circuit's contraband limitation may have little import in practice. The Ninth Circuit held below that officers may inspect text messages and phone logs. Pet. App. 27a. Since this decision, at least one court within the Ninth Circuit has deduced that the contraband rule allows agents to inspect photos stored on electronic devices. *See Adlerstein v. CBP*, 2020 WL 5846600, at *3, *14 (D. Ariz. 2020). And once customs agents are legitimately inspecting any given app, the Ninth Circuit seems to treat the plain-view doctrine as allowing the seizure of any apparent evidence of criminality that they identify. *See* Pet. App. 27a (holding that "[t]he observation that the phone contained no text messages falls comfortably within the scope of a search for digital contraband"); *see generally Coolidge v. New Hampshire*, 403 U.S. 443 (1971).

B. Lower courts have given little attention to various legal considerations that are relevant to how the Fourth Amendment applies to searches of cell phones at the border.

Cell phone searches at the border also implicate various legal issues that have thus far received scant consideration in the lower courts, including: (1) the effect of an arrest on the permissibility of searching phones without warrants, (2) how positive law may inform the Fourth Amendment analysis, (3) whether the expressive character of information on smart phones necessitates heightened

protection from searches, and (4) the effect of data retention on the reasonableness of cell phone searches.

1. Some judges have called for a warrant requirement for at least some searches of cell phones incident to arrest at the border. *See, e.g.*, *United States v. Vergara*, 884 F.3d 1309, 1315 (11th Cir. 2018) (Jill Pryor, J., dissenting); *United States v. Caballero*, 178 F. Supp. 3d 1008, 1017-18 (S.D. Cal. 2016); *United States v. Molina-Isidoro*, 267 F. Supp. 3d 900, 909-10 (W.D. Tex. 2016), *aff'd*, 884 F.3d 287 (5th Cir. 2018). The First Circuit in *Alasaad*, however, did not consider the relevance of an arrest preceding a cell phone search at the border because none of the plaintiffs in that case had been arrested. And the Ninth Circuit's consideration of whether a warrant is required when a person has been arrested was influenced by its pre-*Riley* en banc decision in *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013) (en banc). Pet. App. 17a-19a. Here, the Ninth Circuit relied on the fact of arrest in its discussion of forensic searches but set aside that fact when considering the agents' manual searches of Mr. Cano's phone. *See id.* 27a-30a.

An arrest supports the need for a warrant to conduct any phone search at the border. In *Riley v. California*, 573 U.S. 373, 386 (2014), the Court held that, absent exigent circumstances, officers must "secure a warrant" before searching a phone seized incident to arrest. Once an arrest has been made, the reasons for a warrantless search no longer exist. "[D]ata on the phone can endanger no one," and there is "no longer any risk that the arrestee himself will be able to delete incriminating data from the phone." *Id.* at 387-88. Here too, once a person is arrested and his phone has been seized, there is no risk that he will carry any

digital contraband across the border. In this situation, no justification remains for a border search; all that remains is an "evidence-gathering" purpose to aid the eventual prosecution. *See United States v. Molina-Isidoro*, 884 F.3d 287, 296 (5th. Cir. 2018) (Costa, J., specially concurring). Just as in *Riley*, that purpose can be met by getting a warrant and keeping the phone secure. Indeed, technological advances continue to make getting a warrant "more efficient," *Riley*, 573 U.S. at 401, with some judges issuing them "in as little as five minutes," *Missouri v. McNeely*, 569 U.S. 141, 173 (2013) (Roberts, C.J., concurring in part and dissenting in part).

This case illustrates these realities. Agents seized and secured Mr. Cano's phone over two hours before they initially searched it, and over three hours before they searched it again. *See supra* at 3-4. And all of the pertinent information the agents later found on the phone would have been available if they had waited to obtain the warrant before conducting the searches. *See* Pet. App. 30a.

The Government protests that when agents arrest someone at the border, they may conduct a warrantless search of a "written list of phone numbers" or other tangible written or photographic papers. Pet. 16-17. But this sort of analogy to information that might be found on a phone is exactly what this Court unanimously rejected in *Riley*. Repudiating the Government's contention that searching cell phones is no different than searching physical objects or containers seized incident to arrest, the Court explained that a physical search of papers or photos bears little resemblance to a search of information on a cell phone. *Riley*, 573 U.S. at 400. The rules that govern the former do not control the latter.

2. Nor have the lower courts considered how reference to positive law may inform the constitutionality of the types of searches at issue here. In recent cases, Members of this Court have suggested that Fourth Amendment analyses depend at least in part on "positive law"—that is, statutes and other legal rules historically or presently governing the type of search at issue. *See Carpenter v. United States*, 138 S. Ct. 2206, 2270, 2272 (2018) (Gorsuch, J., dissenting); *Byrd v. United States*, 138 S. Ct. 1518, 1531 (2018) (Thomas, J., concurring). The Fourth Amendment prohibits "unreasonable" searches, and external legal norms can be a good barometer for reasonableness. Indeed, some Justices have felt constrained in their ability to resolve cases without sufficient development of such positive-law arguments. *See Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting); *Byrd*, 138 S. Ct. at 1531 (Thomas, J. concurring).

A comprehensive assessment of positive law here could be illuminating, and perhaps even decisive. Congress has been responsible for passing laws regulating border searches since the Founding. *See Carroll v. United States*, 267 U.S. 132, 151-152 (1925) (reciting history of laws authorizing customs agents to search for contraband). And while Congress has yet to pass legislation specifying substantive rules to govern border searches of electronic devices, there are several longstanding statutes suggesting that a warrant or individualized suspicion of contraband is necessary for such searches.

At least two statutes suggest that such searches are unreasonable without a warrant. First, a customs statute dating to the Founding Era has always required a warrant to search a person's home for items subject to duty, or for evidence relating

to a border offense. *See* An Act to Regulate the Collection of the Duties Imposed by Law on the Tonnage of Ships or Vessels, and on Goods, Wares and Merchandises Imported into the United States, ch. 5, § 24, 1 Stat. 29, 43 (1789); 19 U.S.C. § 1595(a)(1). And in *Riley*, the Court explained that searching someone's cell phone is akin to searching the person's home, as opposed to a container she is carrying. "Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house." *Riley*, 573 U.S. at 396.

Second, customs agents cannot read correspondence contained in international mail without written consent or a warrant. 19 U.S.C. § 1583(c)(2). In fact, customs agents are not even allowed to open sealed mail that weighs sixteen ounces or less. *Id.* § 1583(d). In *United States v. Ramsey*, 431 U.S. 606, 620 (1977), the Court held that the same rules apply to international mail as to items people carry physically across the border. So the restrictions on reading mail that is crossing the border suggest that searches of expressive content on digital devices by customs agents should also require a warrant.

At the very least, customs laws indicate that reasonable suspicion of contraband should be required to search an electronic device at the border. To search trunks or envelopes arriving on vessels at the border, customs officials must have "reasonable cause to suspect there is merchandise which was imported contrary to law." 19 U.S.C. § 482(a). This Court has held that there is good reason for protecting the digital contents of a cell phone at least as stringently as the contents of an envelope or trunk. *See generally Riley*, 573 U.S. 373.

3. This Court has recognized that the Fourth Amendment imposes "special constraints upon searches for and seizures of material arguably protected by the First Amendment." *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 326 n.5 (1979); *see also Marcus v. Search Warrant*, 367 U.S. 717, 731 (1961). And in *Ramsey*, this Court reserved the question whether the border-search exception allows government agents to read written correspondence. 431 U.S. at 623-24 & n.18. Because federal regulations required agents to procure warrants before reading any international correspondence, the Court had "no occasion to decide" whether "the full panoply of Fourth Amendment requirements" should apply where warrantless searches would have a propensity to "chill" speech. *Id.*

In the context of border searches of digital devices, this issue would be even more serious than it would have been in *Ramsey*. Digital devices can hold extraordinary amounts of expressive material—"millions of pages of text, thousands of pictures, or hundreds of videos." *Riley*, 573 U.S. at 394. Furthermore, digital devices may have apps that convey or contain sensitive associational information, such as political or religious affiliations or activities. *See Carpenter*, 138 S. Ct. at 2217; *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

No lower court since *Riley* has seriously considered these arguments. In *Alasaad*, the First Circuit considered a facial First Amendment challenge to CBP's searches of electronic devices. But the First Circuit did not consider how *the Fourth Amendment* should account for the expressive nature of the material stored on cell phones. Allowing lower courts to grapple with this issue in the first instance would ultimately aid this Court.

4. Finally, the lower courts have not fully considered how the Government's policy of retaining data from warrantless electronic border searches might affect the reasonableness of such searches themselves. In *Maryland v. King*, 569 U.S. 435, 443-44 (2013), the Court upheld a state policy of taking DNA samples from arrestees, noting that the state destroyed the samples if the charges were unsupported by probable cause or if a criminal prosecution did not result in conviction. The information found on cell phones is similarly highly sensitive. Yet it appears the Government retains it even when no evidence of criminal activity is found, sometimes for years on end. *See, e.g.*, CBP, DIRECTIVE NO. 3340-049A, BORDER SEARCH OF ELECTRONIC DEVICES § 5.5.1.2 (2018); ICE, DIRECTIVE NO. 7-6.1, BORDER SEARCHES OF ELECTRONIC DEVICES § 8.5(1)(b) (2009); DHS, NO. PIA-053(a), PRIVACY IMPACT ASSESSMENT FOR THE U.S. BORDER PATROL DIGITAL FORENSICS PROGRAMS 8 (2020).

If, long after travelers have come and gone from the border, the Government may still trawl through "a digital record of nearly every aspect of their lives," *Riley*, 573 U.S. at 395, that may tip the balance in a reasonableness analysis. Seizing and storing such information for future use makes the violation of the traveler's privacy especially severe. Years later, the Government might analyze the information with tools or techniques that do not yet exist or use it for reasons having nothing to do with enforcing border-related laws. *See Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).

C. Completing the shift to cloud storage will alter the technological landscape in relevant ways.

In addition to legal issues, evolving technological developments in cloud storage counsel caution before the Court attempts to establish any constitutional rules governing searches of digital devices at the border. As the Court previously has observed, "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." *City of Ontario v. Quon*, 560 U.S. 746, 759 (2010); *see also Packingham v. North Carolina*, 137 S. Ct. 1730, 1736 (2017). Such is the case here with respect to cloud computing—that is, the ability to store data on a remote server and retrieve it as necessary, rather than storing it on the device itself.

The issue of cloud storage complicates how—or even whether—the border-search exception applies to cell phones. The exception is rooted in the government's authority to stop and examine "persons and property *crossing into this country*." *Ramsey*, 431 U.S. at 616 (emphasis added). The border-search power, therefore, extends only to people or things "enter[ing] into our country from outside." *Id.* at 619. Cloud data, however, does not "enter" the country with the traveler at all. As such, it must be off-limits during any border search. Searching "files stored in the cloud" on a seized cell phone would be "like finding a key in a suspect's pocket and arguing that it allow[s] law enforcement to unlock and search a house." *Riley*, 573 U.S. at 397.

As cloud technology develops and becomes more enmeshed in smartphone interfaces, there will be a higher risk that border agents who search cell phones will

search cloud data. Such searches can occur inadvertently because information stored in the cloud "may appear as a seamless part of the digital device when presented at the border." *Cotterman*, 709 F.3d at 965; *see also Riley*, 573 U.S. at 397-98. Indeed, while current CBP policies forbid agents from searching cloud data, the agency has struggled in the past to implement such directives. *See* DHS, OFFICE OF INSPECTOR GENERAL, OIG-19-10, CBP'S SEARCHES OF ELECTRONIC DEVICES AT PORTS OF ENTRY 6 (2018). On the other hand, if border agents are able in the future to avoid searching cloud information on phones, any border-search authority to inspect data stored locally will become increasingly inconsequential, as less and less data is actually stored "on" the phone. Either way, the Court should allow the paradigm shift to cloud computing to come to fruition, and wait for border agencies to respond to that reality, before establishing any new rules in this area. Otherwise, the Court risks any new judicial pronouncements becoming quickly outdated.

D. Additional percolation would create breathing space for Congress.

Members of this Court have suggested in cases involving technological change that "the best solution to privacy concerns may be legislative." *Jones*, 565 U.S. at 429 (Alito, J., concurring, joined by Ginsburg, Breyer, and Kagan, JJ.); *see also Riley*, 573 U.S. at 407-08 (Alito, J., concurring in part and concurring in the judgment). That may well be the case here.

Congress's power to regulate foreign commerce gives it an important role in regulating "searches of persons or packages at the national borders." *United States v. 12 200-Ft. Reels of Super 8mm. Film*, 413 U.S. 123, 125 (1973). Congress also has exercised this power in response to the modern ubiquity of cell phones and

developments in data storage. The Trade Facilitation and Trade Enforcement Act of 2015 requires that CBP establish standard operating procedures for "searching, reviewing, retaining, and sharing information" on electronic devices at ports of entry. Pub. L. No. 144-125, 130 Stat. 122, 205. The statute further requires that these procedures be updated every three years. *Id.* at 206. Congress also recently enacted legislation dealing with personal privacy for data stored in the cloud and the rules for the Government to obtain such data. *See* CLOUD Act, Pub. L. No. 115-141, 132 Stat. 348, 1213-25 (2018).

Congress has also shown interest in passing new legislation that could directly affect, or even moot, the specific question presented in this case. In 2019, multiple bills were proposed that would significantly restrict searches and seizures of electronic devices at the border, including by imposing a warrant requirement for any search of the devices of a United States citizen or lawful permanent resident. *See* S. 2694, 116th Cong. (2019); S. 1606/H.R. 2925, 116th Cong. (2019). While none of these bills was enacted into law, there has been "an array" of bipartisan support for such legislation. *Examining Warrantless Smartphone Searches at the Border: Hearing Before the Subcomm. on Fed. Spending Oversight & Emergency Mgmt. of the S. Comm. on Homeland Sec. & Gov. Affairs*, 115th Cong. 10 (2018).

III. There is no immediate need to address how the border-search doctrine applies to cell phones.

A. The Government can use other means to conduct investigations at the border.

The Government claims that the decision below "disrupts the day-to-day work of border officials." Pet. 13. But that is not the case. The Ninth Circuit's

contraband rule will often pose no obstacle to routine searches at the border, for several reasons.

1. Individuals often consent to searches of their phones. Experts estimate that ninety percent of all warrantless police searches are consent searches. Alafair S. Burke, *Consent Searches and Fourth Amendment Reasonableness*, 67 Fla. L. Rev. 509, 511 (2015). People at the border may be more willing to consent to avoid further inconvenience or delays to their travel. *See, e.g.*, *United States v. Vergara*, 884 F.3d 1309, 1311 (11th Cir. 2018) (traveler acceded to search); *United States v. Ramirez*, 2019 WL 3502913, at *18 (W.D. Tex. 2019) (same). And if an individual consents to a search, the Ninth Circuit's scope limitation is not implicated at all.

2. As noted above, the Government "does not construe the [Ninth Circuit's] decision to foreclose reliance on" national security grounds for border searches. Pet. 19 n.*. And CBP, the primary agency tasked with conducting searches at ports of entry, explicitly recognizes national security concerns as an independent justification for border searches. CBP, DIRECTIVE NO. 3340-049A, BORDER SEARCH OF ELECTRONIC DEVICES § 5.1.4 (2018). The same is presumably true when other sorts of exigent circumstances arise. *See Missouri v. McNeely*, 569 U.S. 141, 149 (2013).

3. In many instances, the Government can get—and is already getting—warrants for digital searches at the border. Federal defender offices report that, since 2018, border agents within the Ninth Circuit have been procuring warrants before searching the phones of arrestees at ports of entry. And the Government has

not shown that the process of procuring a warrant has hampered its investigatory activities at the border.

B. The Ninth Circuit's contraband rule would not prevent the Government from dealing with the hypothetical scenarios it raises.

The Government nonetheless raises two types of hypotheticals to suggest that the search authority it seeks here is necessary. But both types underscore that the Ninth Circuit's digital contraband limitation poses little obstacle to the Government's ability to identify and investigate border-related crime.

In the first type, border agents have "already discovered drugs (or other contraband)" but are in a race against the clock to accomplish "the rapid interdiction of other drugs." Pet. 21. But if such time-sensitive scenarios truly arise, the exigency exception to the warrant requirement would presumably allow border agents to conduct any necessary electronic device search.

In the second type, border agents have not yet found contraband, but an electronic device search is purportedly necessary to learn that the device owner or another traveler in close proximity is transporting drugs. Pet. 20. But the Government overstates the importance in this scenario of conducting a warrantless search of a cell phone. Border agents already employ tools—such as narcotics-detecting dogs, Pet. 5, and compulsory x-rays or scans, *see, e.g.*, *United States v. Molina-Isidoro*, 884 F.3d 287, 289 (5th Cir. 2018)—that are much more likely than a fishing expedition on a phone to detect the presence of physical contraband at the border. Indeed, those methods enabled the discovery of the only contraband found in this case.

Moreover, any need for border agents to rely on warrantless device searches in these scenarios will soon disappear. A plan to digitally scan the physical contents of all commercial and passenger vehicles crossing the border—not just those referred to secondary inspection—has already been signed into law. *See* Securing America's Ports Act, Pub. L. No. 116-299, 134 Stat. 4906 (2021). Accordingly, border authorities will scan every car in the "drug-smuggling convoy," Pet. 20, for physical contraband regardless.

In any event, if one day a case like the Government's hypotheticals were to arise—where the Government can claim that it was left with no means other than a suspicionless device search at the border to identify an impending threat of contraband—the Court can assess the issue then, with a concrete factual record before it.

IV. The Ninth Circuit correctly held that the Fourth Amendment was violated here.

A. The Ninth Circuit's scope holding is sound.

Notwithstanding certain broad language the Government quotes from past opinions, the border-search exception (at least as applied to United States citizens and lawful permanent residents) is properly limited to efforts to detect contraband.

1. The border-search exception is based on the need to enforce customs laws and to prevent illegal importation of goods. *See United States v. 12 200-Ft. Reels of Super 8mm Film*, 413 U.S. 123, 125-26 (1973). Colonial-era law that permitted customs agents to search ships at the border focused on collecting duties and driving revenue. *See* Laura K. Donohue, *Customs, Immigration, and Rights:*

Constitutional Limits on Electronic Border Searches, 128 Yale L.J.F. 961, 972-74 (2019). Such law during the Founding Era was also concerned with the enforcement of duties. *See United States v. Flores-Montano*, 541 U.S. 149, 153 (2004). Indeed, the exception has existed "since the beginning of our Government" to enable federal officials "to regulate the collection of duties and to prevent the introduction of contraband into this country." *Id.* (quoting *United States v. Montoya de Hernandez*, 473 U.S. 537 (1985)); *see also* An Act to Provide More Effectually for the Collection of the Duties Imposed by Law on Goods, Wares and Merchandise Imported into the United States, and on the Tonnage of Ships or Vessels, ch. 35, §§ 48-51, 1 Stat. 145, 170 (1790).

The Government notes that the Court has also described the border-search doctrine as partially grounded in protecting "territorial integrity." Pet. 18 (quoting *Flores-Montano*, 541 U.S. at 153). And the Government quotes the Court's decades-old statement that border searches "have been considered to be 'reasonable' by the single fact that the person or item" was crossing our border. Pet. 18 (quoting *Ramsey*, 431 U.S. at 619). But that language does not explain the Court's suggestion in *Montoya de Hernandez* that at least some highly intrusive border searches may require warrants or reasonable suspicion of contraband. *See* 473 U.S. at 541 n.4. And the fact remains that the Court has never upheld a border search for anything other than contraband. Pet. App. 24a-25a.

In light of this history and precedent, the Ninth Circuit correctly held that border searches must be limited in scope to inspections for contraband. A search

like the one here that continues even after it is clear a seized item does not contain contraband is not a valid border search.

2. Contrary to the Government's contention, the Ninth Circuit's holding here is fully consistent with *Warden v. Hayden*, 387 U.S. 294 (1967).

Hayden held that when police officers are conducting an "otherwise permissible" search of a place, they may seize "mere evidence" of criminality that they come upon. 387 U.S. at 301, 306. In so holding, the Court backed away from its prior suggestion in *Boyd v. United States*, 116 U.S. 616 (1886), and other cases that private papers could never be inspected or seized merely for evidentiary purposes.

The Ninth Circuit held here that a border search is not valid in the first place when contraband could not be found in the place being searched. This holding does not resurrect any portion of *Boyd* that is no longer good law. The Ninth Circuit merely applied the time-honored rule that a warrantless search "must be strictly tied to and justified by the circumstances which rendered its initiation permissible." *Terry v. Ohio*, 392 U.S. 1, 19 (1968) (internal quotation marks and citation omitted) (frisk for weapons); *see also Riley v. California*, 573 U.S. 373, 382 (2014) (search of a phone incident to arrest); *Arizona v. Gant*, 556 U.S. 332, 343 (2009) (search of a car incident to arrest); *Maryland v. Buie*, 494 U.S. 325, 335 (1990) (a "protective sweep" of a home is "not a full search of the premises, but may extend only to a cursory inspection of those spaces where a person may be found"). As explained above, warrantless border searches are permissible only to prevent contraband from crossing into the country.

The Government also cites *Hayden* for the proposition that any distinction between "mere evidence" and "instrumentalities, fruits of crime, or contraband" is arbitrary and difficult to administer. Pet. 21-22 (quoting *Hayden*, 387 U.S. at 301). But that is clearly untrue at the border. Federal customs statutes have long limited which agents may search for which items in precisely this way. For example, a customs agent stopping and boarding a vessel may "search any trunk or envelope, wherever found" only when "he may have a reasonable cause to suspect there is merchandise which was imported contrary to law." 19 U.S.C. § 482.

B. The Fourth Amendment was violated here for other reasons as well.

Finally, a respondent is entitled to defend the judgment below on alternative legal grounds—especially where, as here, the court of appeals considered those arguments. *See, e.g.*, *Bennett v. Spear*, 520 U.S. 154, 166-67 (1997). Here, there are two additional reasons besides the Ninth Circuit's scope holding why the searches of Mr. Cano's phone violated the Fourth Amendment.

1. A warrant should be required to search a digital device at the border—at least where, as here, federal agents have arrested the phone's owner and are searching for evidence of the crime of arrest. Under *Riley*, the Court must balance the need to search an electronic device seized incident to arrest against the privacy implications of doing so without a warrant. 573 U.S. at 385-86. As the Ninth Circuit recognized, once an individual is arrested and his cell phone has been seized, there is no need to search the phone without procuring a warrant. Pet. App. 30a. And *Riley* establishes that the impingement on privacy of even a manual search of a cell

phone is severe. *See* 573 U.S. at 394. Consequently, the balance here—just as in *Riley*—dictates the need for a warrant.

What is more, positive law dating back to the Founding has always required warrants to search homes as part of investigations of border-related crimes. *See supra* at 17-18. And as this Court recognized in *Riley*, searching a person's phone is properly analogized to the search of a home, not the search of a container the person is carrying. 573 U.S. at 396-97. Lest there be any doubt, the expressive nature of the material at issue and the Government's retention policies reinforce the need for warrants in this situation. *See supra* at 19-20.[2]

2. At a minimum, any search of a cell phone—manual or forensic—is so intrusive as to require reasonable suspicion of digital contraband. In *Montoya de Hernandez*, the Court held that reasonable suspicion that a traveler is "smuggling contraband" in her alimentary canal is required to seize her and monitor her bowel movements. 473 U.S. at 541. The Court has twice reserved the related question whether certain border searches are so "highly intrusive" that they are subject to a requirement of "reasonable suspicion, probable cause, or a warrant." *Flores-Montano*, 541 U.S. at 152 (quoting *Montoya de Hernandez*, 473 U.S. at 541 n.4).

The Ninth Circuit extrapolated from this precedent that because a forensic search of a cell phone is "highly intrusive," it requires reasonable suspicion of

---

[2] A warrant is even more necessary for a search of messages arriving on the phone after it was seized. Here, at least one WhatsApp message introduced at trial was received hours *after* the customs agents seized Mr. Cano's phone at the border. Pet. App. 5a; C.A. E.R. 1064. The fact that this message did not exist when Mr. Cano presented himself at the border means that reading the message cannot be justified under the border-search exception to the warrant requirement.

contraband. Pet. App. 29a. For the reasons the Court recognized in *Riley*, the same should be true of manual searches of cell phones. *See Riley*, 573 U.S. at 394-96; *see also United States v. Kolsuz*, 890 F.3d 133, 145-46 (4th Cir. 2018). Indeed, in the proceedings below, the Government contended that even a search using Cellebrite software is a manual search. Pet. App. 30a n.12. If, as the Government suggests, a search as intrusive as the Cellebrite search performed here is "manual," it is all the more apparent that at least reasonable suspicion of contraband must be required for all cell phone searches.

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be denied.

Respectfully submitted,

Jeffrey L. Fisher
STANFORD LAW SCHOOL
SUPREME COURT LITIGATION
CLINIC
559 Nathan Abbott Way
Stanford, CA 94305

Harini P. Raghupathi
Counsel of Record
FEDERAL DEFENDERS
OF SAN DIEGO, INC.
225 Broadway, Suite 900
San Diego, CA 92101
(619) 234-8467
Harini_Raghupathi@fd.org

May 12, 2021