No. _____

In the Supreme Court of the United States

ALVARO CASTILLO, JR., *PETITIONER*,

v.

UNITED STATES OF AMERICA, *RESPONDENT*

PETITION FOR WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FIFTH CIRCUIT

MAUREEN SCOTT FRANCO
Federal Public Defender

KRISTIN L. DAVIDSON
Assistant Federal Public Defender
Western District of Texas
300 Convent Street, Suite 2300
San Antonio, Texas 78205
(210) 472-6700
(210) 472-4454 (Fax)
Kristin_Davidson@fd.org

Counsel of Record for Petitioner

QUESTION PRESENTED FOR REVIEW

Whether, or under what circumstances, the Fourth Amendment permits customs officers to conduct a warrantless search of the digital contents of a person's cell phone seized at the U.S. border?

No. _____

In the Supreme Court of the United States

ALVARO CASTILLO, JR., *PETITIONER*,

v.

UNITED STATES OF AMERICA, *RESPONDENT*

PETITION FOR WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FIFTH CIRCUIT

Petitioner Alvaro Castillo, Jr. asks that a writ of certiorari issue to review the opinion and judgment entered by the United States Court of Appeals for the Fifth Circuit on June 19, 2023.

PARTIES TO THE PROCEEDING

The caption of this case names all parties to the proceeding in the court whose judgment is sought to be reviewed.

RELATED PROCEEDINGS

- *United States v. Castillo*, No. 4:19-cr-00780-DC (W.D. Tex. May 4, 2021) (judgment of conviction)
- *United States v. Castillo*, No. 21-50406 (5th Cir. June 19, 2023)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Regulations

Other Authorities

OPINION BELOW

A copy of the opinion of the court of appeals, *United States v. Castillo*, No. 21-50406 (5th Cir. June 19, 2023), is reproduced at Pet. App. 1a–7a. The opinion is reported as *United States v. Castillo*, 70 F.4th 894 (5th Cir. 2023).

JURISDICTION OF THE SUPREME COURT OF THE UNITED STATES

The opinion and judgment of the United States Court of Appeals for the Fifth Circuit were entered on June 19, 2023. Justice Alito granted Petitioner's motion to extend the time for filing a petition for writ of certiorari to October 17, 2023. *See Castillo v. United States*, No. 23A193. The Court has jurisdiction to grant certiorari under 28 U.S.C. § 1254(1).

CONSTITUTIONAL PROVISION INVOLVED

The Fourth Amendment to the U.S. Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV.

STATEMENT

This case presents the pressing question of whether the Fourth Amendment protects against the government's warrantless search of the digital contents of a cell phone seized at the U.S. border.

1. Petitioner was traveling south from Colorado with his adult nephew and his nephew's friend. Around midnight on October 12, 2019, they crossed the U.S.-Mexico border at the international bridge from Presidio, Texas, to Ojinaga, Chihuahua, Mexico, driving Petitioner's recreational vehicle (RV), behind which they towed a passenger car. Mexican authorities told them they needed to cross the RV and car separately. To do this, they made a U-turn between the nations' checkpoints to reenter the United States where they could separate the vehicles. *See* ROA.103–04.[1]

Based on the time of night and size of the RV, Petitioner was directed by a U.S. Customs and Border Patrol (CBP) agent to drive to the secondary lane for reentry into the United States. The three men told the agent what the Mexican authorities had instructed them to do, and they presented their valid identification documents. They were held in the Passport Control Services lobby while another agent searched their vehicles. *See* ROA.103–04.

---

[1] "ROA" refers to the pagination of the record on appeal filed in the Fifth Circuit Court of Appeals.

In the RV, agents found a .357 revolver wrapped in packing foam and taped between two frying pans inside the oven, as well as ammunition inside a pressure cooker that was taped shut. A personal-use amount of marijuana was found inside a suitcase. Petitioner, who claimed ownership of all property, was removed from the Passport Lobby, taken to a secure, windowless holding cell, and handcuffed to a bench. *See* ROA.104, 348–49.

Homeland Security Investigation Agent Tim Henderson was called to investigate. He confirmed Petitioner's ownership of the revolver and searched for any paperwork that might indicate an ongoing smuggling venture. He found none. *See* ROA.350–52, 363.

Agent Henderson did not suspect that Petitioner's cell phone contained contraband. ROA.364. But he wanted to search it for evidence of a smuggling venture. ROA.352. Because the cell phone was locked, Agent Henderson demanded that Petitioner tell him the passcode. He did not ask for consent, nor administer *Miranda* warnings. Petitioner told him the passcode. ROA.353, 369–70, 373.

Agent Henderson searched through the text messages, other communication apps, such as WhatsApp and Snapchat, recent calls, and may have also searched Petitioner's emails. But he found no evidence of a crime. *See* ROA.354–57, 364, 367.

When Agent Henderson opened the photos folder on the cell phone, however, he discovered photographs and videos that he considered to be child pornography. Based on this discovery, the remainder of the electronic devices, including cell phones, tablets, laptops, and thumb drives, were manually and forensically searched, yielding additional images of child pornography and specific locations where the images were recorded. *See* ROA.335–46, 364–65, 368, 692–96.

The government's investigation discovered at least four separate videos of an adult male attempting to or sexually assaulting minor females who were asleep. *See* ROA.666, 670–72, 697–98, 711, 713, 715–19, 721–27. The location data indicated the videos were recorded around May 18 and 21, 2018, in Guatemala. ROA.680–81, 727–28. A CBP agent contacted the minors in Guatemala, who confirmed that they were the victims in the videos. Other evidence indicated that Petitioner was in Guatemala between May 18 and 21, 2018. ROA.888, 890–91, 917.

2. Petitioner was charged by a second superseding indictment with three counts of producing of child pornography, in violation of 18 U.S.C. § 2251(a); one count of the attempted production of child pornography, in violation of 18 U.S.C. 2251(a); and one count each of transporting and possessing child pornography, in violation of 18 U.S.C. §§ 2252(a)(1) and (a)(4), respectively.

Petitioner moved to suppress the evidence obtained from the manual search of his cell phone and its tainted fruits. *See* ROA.50–80, 110–14. Relying on *Riley v. California*, 573 U.S. 373 (2014), Petitioner argued that the Fourth Amendment's warrant requirement applies to searches of cell phones at the border, and there was no probable cause that the cell phone contained contraband. Also, Agent Henderson's demand for Petitioner's passcode without first administering *Miranda* warnings, violated his Fifth Amendment right. Because the discovery of the child pornography would have been impossible without Castillo's passcode, that evidence ought to have been suppressed.

The district court denied Petitioner's motion, concluding that *Riley* did not extend to the search of cell phones at the border. ROA.138–63. The court rejected the need to determine whether the search of Petitioner's cell phone was a routine or non-routine border search, but reasoned that, if any amount of suspicion was required, at most agents need reasonable suspicion that criminal activity was afoot, which Agent Henderson established. It also found that Petitioner's Fifth Amendment right had been violated. It suppressed the passcode but not the physical evidence discovered on the cell phone.

3. A jury found Petitioner guilty on all counts. The district court imposed a total sentence of 720 months' imprisonment, followed by a life term of supervised release.

4. The Fifth Circuit affirmed. It held that, under the border search exception to the Fourth Amendment, the manual search of a cell phone at the border is a routine search for which no individualized suspicion is required. Pet. App. 6a–7a. The court recognized that "[t]he circuits are divided" over the application of the border-search exception to forensic searches of cell phones. *Id.* But it concluded that no circuits require warrants or reasonable suspicion for manual cell phone searches at the border,[2] and "adopt[ed] that consensus." *Id.*

---

[2] The Fifth Circuit subsequently declined to extend the Fourth Amendment's warrant requirement to forensic cell phone searches. In *Malik v. Dept. of Homeland Security*, 78 F.4th 191 (5th Cir. 2023), the court explained that its "precedent does not currently require a warrant for cell phone searches at the border," that individualized suspicion need not be present for manual searches, and that reasonable suspicion, and not probable cause, is the proper standard for forensic searches. *Id.* at 201.

REASONS FOR GRANTING THE WRIT

Federal courts are divided over whether, and under what circumstances, the Fourth Amendment tolerates the warrantless search of the digital contents of a cell phone at the U.S. border or border equivalent. This Court should use this case, which presents the preserved issue with a comprehensive fact pattern, to resolve the conflict and hold that the warrantless search of digital data at the border is unreasonable under Fourth Amendment.

I. Federal courts are divided over whether, or to what extent, the Fourth Amendment protects against the warrantless search of a cell phone at the U.S. border.

A. Background.

1. The Fourth Amendment, and its protections against "unreasonable searches and seizures," was "the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era[.]" *Riley*, 573 U.S. at 403. Those unrestricted searches were often executed by British customs officers who then "rummage[d] through homes in an unrestrained search for evidence of criminal activity." *Id.*; *see generally* WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 602–1791, at 253–62 (2009) (describing the repugnance that colonial Americans felt toward searches and seizures by British customs officers by

1760). Ordinarily, government searches to uncover criminal wrongdoing require a warrant supported by probable cause. *Riley*, 573 U.S. at 382. "In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement." *Id*.

One of those exceptions is the border search doctrine. As early as 1886, the Court took note of the potential relevance of a customs statute passed by the First Congress to the Fourth Amendment's original meaning. *Boyd v. United States*, 116 U.S. 616, 623 (1886). That Act authorized warrantless searches at the waterline of ships and, upon disembarkation, of their cargoes. Act of July 31, 1789, ch. 5, §§ 23, 24, 1 Stat. 29, 43; *see also* W. CUDDIHY, THE FOURTH AMENDMENT at 746. Yet, the scope of those searches had limits. Customs officers were authorized to enter "any ship or vessel" and search for "goods, wares or merchandise" subject to duty without a warrant if they had "reason to suspect any goods, wares or merchandise subject to duty" were concealed. Act of July 31, 1789, ch. 5, § 24, 1 Stat. 29, 43. In order "to open and examine" any package, a customs officer had to suspect fraud and could only open and examine the packages in "the presence of two or more reputable merchants." Act of July 31, 1789, ch. 5, § 23, 1 Stat. 29, 43. If no fraud was detected, the officer had to repack the goods and pay the costs of their examination. *Id*.

The modern framework for analyzing the border search exception to the Fourth Amendment emanates from *United States v. Ramsey*, 431 U.S. 606, 620 (1977). Citing the First Congress, the Court recognized that the "border-search exception is grounded in the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country." *Id.* at 620. That includes the power to seize and search "all persons coming into the United States," as well as any "vehicle, beast, or person" upon which an officer suspects there is contraband or merchandise that is subject to duty. *See* 19 U.S.C. §§ 482, 1582. The Court reasoned that the border-search exception is "a longstanding historically recognized exception" that is "similar" to the "search incident to lawful arrest exception" in *United States v. Robinson*, 414 U.S. 218 (1973). *Id.* at 622. Thus, it was reasonable under the Fourth Amendment for customs officials to open envelopes without a warrant as long as they had reason to believe they contained other than correspondence. *Ramsey*, 431 U.S. at 624. While only reasonable suspicion was needed to confirm whether the physical contents of envelopes contained merchandise or contraband, the reading of any correspondence remained forbidden without a warrant. *Id.* at 624; *see also* 19 C.F.R. § 145.3 (2021).

However, "[r]outine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant." *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). The Court briefly distinguished between routine and non-routine inspections when it held that that "the detention of a traveler at the border, beyond the scope of a routine customs search and inspection"—overnight detention to see if a bowel movement would produce drugs—must be "justified at its inception" by "reasonabl[e] susp[icion] that the traveler is smuggling contraband in her alimentary canal." *Id*. at 541.

The Court later rejected that the term "routine" fashioned a new balancing test for the suspicionless disassembly of a gas tank. *United States v. Flores-Montano*, 541 U.S. 149, 152–53 (2004). Whatever "the reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of a person—dignity and privacy interests of the person being searched—simply do not carry over to vehicles." *Id*. at 152. That is because "[i]t is difficult to imagine how the search of a gas tank, which should be solely a repository for fuel, could be more of an invasion of privacy than the search of the automobile's passenger compartment." *Id*. at 154.

2. There is no precise guidance from the founding era regarding the Fourth Amendment's application to modern technologies and the

"quantitative and qualitative" differences between modern cell phones and "other objects" that might be carried on a person. *Riley*, 573 U.S. at 393. Thus, new technologies require the Court to reexamine "whether to exempt a given type of search from the warrant requirement by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests. *Id*. at 385–86; *see also id*. at 407 (Alito, J., concurring in part and concurring in judgment) (calling for "a new balancing of law enforcement and privacy interests" in the modern digital era of cell phones).

The Court has rejected a "mechanical interpretation" of the Fourth Amendment "[a]s technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes," in order to "'assure[ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018) (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (holding that use of thermal imaging to detect heat radiating from side of defendant's home was a search). The Court has confronted the crucial question regarding the application of the Fourth Amendment in the modern digital age in three cases. *See Carpenter*, 138 S. Ct. 2206 (warrant

required for cell phone location information obtained from a third-party wireless carrier); *Riley*, 134 S. Ct. 2473 (2014) (warrant required for search of cell phone seized incident to lawful arrest); *United States v. Jones*, 565 U.S. 400 (2012) (tracking car with GPS device is a Fourth Amendment search).

In *United States v. Jones*, the Court held that attaching a GPS device to a vehicle and tracking its movements constitutes a search under the Fourth Amendment. 565 U.S. at 404. The Court made clear that novel digital surveillance technologies not in existence at the framing of the Fourth Amendment do not escape the Fourth Amendment's reach. *Id.* at 406–07; *id.* at 430 (Alito, J., concurring in the judgment) ("[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.").

In *Riley*, the Court addressed Americans' privacy rights in the contents of their cell phones, unanimously holding that warrantless, manual search of the contents of a cell phone incident to a lawful arrest violates the Fourth Amendment. 573 U.S. at 403. In so doing, the Court cautioned against an analogue test that compares digital data to physical records, which risks causing "a significant diminution of privacy." *Id.* at 400–01. That is because the digital data contained on

a cell phone is quantitatively and qualitatively different than any item typically carried on a person when they travel. *See id.* at 393–99. The digital data on cell phones contain the "privacies of life," even more so at times than the contents of a home. *Id.* at 396, 403. Thus, the "answer to the question of what police must do before searching a cell phone seized incident to arrest is accordingly simple—get a warrant." *Id.* at 403.

The Court confronted another new technological phenomenon in *Carpenter*—how to apply the Fourth Amendment to "the ability to chronicle a person's past movements through the record of his cell phone signals." 138 S. Ct. at 2217. It held that the third-party doctrine did not except cell phone location records from the Fourth Amendment's warrant requirement. *Id.* at 2221. That holding again turned on "the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection." *Id.*

This case presents an important next step in the ongoing effort to reconcile enduring Fourth Amendment principles with the reality of a modern digital world. Whether it is unreasonable under the Fourth Amendment for customs officials to rummage indiscriminately through a traveler's cell phone—and the "privacies of life" it contains—without a warrant is a question only this Court can answer.

B. The conflict.

The federal courts are divided over how to balance an individual's heightened privacy interests in digital data, established in *Riley*, and the justifications that permit the warrantless search of other physical containers or personal effects at the border. Only the Court can clarify the scope of the Fourth Amendment's protections in this context.

1. The Ninth Circuit distinguishes between a search for evidence and a search for digital contraband. It holds that searches by border officials for evidence relating to a crime (such as the search here) require a warrant, because border agents "have no general authority to search for a crime." *United States v. Cano*, 934 F.3d 1002, 1016–17 (9th Cir. 2019). The government's interest in obtaining evidence—as opposed to interdicting contraband or other unwanted items or persons—is not materially different at the border than elsewhere. *Id.* at 1016–19.

Cano's other holding—that warrantless searches for digital contraband are permissible, whether without any heightened suspicion in the case of "manual" searches (scrolling through someone's phone), or with reasonable suspicion in the case of "forensic" searches, *id.* at 1012–16—conflicts with *Riley*. While the Ninth Circuit acknowledged *Riley*, it applied the standard it had previously established in *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013) (en banc), reasoning that *Riley* did not apply to the border search doctrine. *Id.* at 1015.

Focusing specifically on child pornography as the kind of digital contraband contained on a cell phone, the Ninth Circuit analogized that "photos stored [on a cell phone are] the equivalent of photos, magazines, and books." *Id*. at 1014. But *Riley* expressly rejected such a mechanical analogy between digital data and physical objects. *Riley*, 573 U.S. at 397–98. Thus, the Ninth Circuit failed to square digital contraband with the historically grounded interest in interdicting physical contraband. Such an "analogy crumbles entirely" given the frequency with which cloud computing stores information elsewhere. *See id.* at 397. That is because stopping a cell phone at the border does not mean stopping the data it contains. *See* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 365–77 (2015) (discussing the challenges of diffusion of data poses to concepts of territoriality).

The Fourth Circuit has applied similar logic as the Ninth Circuit, reasoning that a warrantless search of a cell phone at the border is impermissible absent some "nexus" between the government's interests in protecting the border and the search. *United States v. Kolsuz*, 890 F.3d 133, 143 (4th Cir. 2018). Such a "nexus" can be satisfied not just by the phone containing actual digital contraband but also by its containing evidence of a border-related violation. *Id.*, 890 F.3d at 143 (holding that agents had reasonable suspicion of criminal activity to

support the forensic search of phone data). But "the Government may not invoke the border exception on behalf of its generalized interest in law enforcement and combatting crime." *United States v. Aigbekaen*, 943 F.3d 713, 720–21 (4th Cir. 2019) (holding that warrantless forensic search of digital data based on investigation into domestic crimes was unconstitutional).

The Ninth and Fourth Circuits are in "tension" with one another. *Cano*, 934 F.3d at 1017. According to the Ninth Circuit, the Fourth Circuit effectively enlarged the border search exception by transforming a warrant-exception based on the government's interest in preventing the introduction of unwanted persons or things into an interest in "search[ing] for evidence of contraband that is not present at the border." *Id.* at 1018. Just as that interest cannot support the government's conducting a warrantless search of a person's house simply because it believes it may contain evidence of a crime, it does not support allowing the Government to conduct warrantless searches of cell phones for evidence of border-related crimes. *Id*. (quoting *Boyd,* 116 U.S. at 622–23).

2. In sharp contrast with the limits articulated by the Ninth and Fourth Circuits, the Fifth Circuit joined the extreme anything-goes approach of the First and Eleventh Circuits. These circuits hold that

the government may search cell phones at the border without a warrant and without any heightened requirement of nexus between the search and the government's interests in preventing the entry of unwanted persons or items. *See Alasaad v. Mayorkas*, 988 F.3d 8, 21 (1st Cir. 2021); *United States v. Touset*, 890 F.3d 1227, 1232 (11th Cir. 2018); *see also Castillo*, Pet. App. 6a–7a.

The First Circuit distinguished *Riley* by stating that "[t]he search incident to arrest warrant exception is premised on protecting officers and preventing evidence destruction, rather than on addressing border crime." *Alasaad*, 988 F.3d at 21. It emphasized that the "border search exception's purpose is not limited to interdicting contraband; it serves to bar entry to those 'who may bring anything harmful into this country' ... [including] 'communicable diseases, narcotics, or explosives.'" *Id*. at 20.

The Eleventh Circuit held that warrants are never required to search cell phones at the border. *United States v. Vergara*, 884 F.3d 1309, 1311 (11th Cir. 2018). It relied heavily on the example of "digital contraband," such as child pornography, to hold that the warrantless, suspicionless search of a cell phone at the border is reasonable. *Touset*, 890 F.3d at 1232–33. It brushed aside this Court's reasoning in *Riley* concerning the unique privacy implications of cell phone searches and noted its conflict with the Ninth and Fourth Circuits.

Id. at 1234–35. It argued instead that "it does not make sense to say that electronic devices should receive special treatment because so many people now own them or because they can store vast quantities of records or effects" since "[t]he same could be said for a recreational vehicle filled with personal effects or a tractor-trailer loaded with boxes of documents." *Id*. at 1233–34; *see also Vergara*, 884 F.3d at 1312–13.

Yet this Court made clear that the storage capacity and pervasive use of cell phones in every aspect of users' lives make them qualitatively and quantitatively different from the sorts of possessions or records a person might carry with her. *Riley*, 573 U.S. at 393. While *Riley* made that observation in the context of considering the kinds of objects a person might have on their person or perhaps in their car at the time of an arrest, the fundamental point—that a cell phone carries far more and far more sensitive information than would historically have been contained in carriable physical objects—also applies at the border.

The Eighth Circuit recently indicated its likely agreement with the First and Eleventh Circuits, but declined to definitively resolve whether there is any nexus requirement. *United States v. Xiang*, 67

F.4th 895, 900–01 (8th Cir. May 5, 2023).[3] It distinguished *Riley* on the barebones basis that it "involved a different Fourth Amendment exception, searches incident to arrest," without explaining why the logic of *Riley* does not apply in the border context. *Id*. at 899.

3. A district court recently surveyed and rejected the circuits' different approaches to the border search exception's application to digital date, hewing closely to the logic of *Riley* and holding that the warrantless search of a cell phone seized at the border was unconstitutional.[4] *United States v. Smith*, No. 22-CR-352, 2023 WL 3358357, at *7, 11 (S.D.N.Y. May 11, 2023). The court applied "the logic and analysis of *Riley* to the border context," and concluded that "the border search exception cannot support its extension to warrantless cell

---

[3] The Tenth Circuit has also summarily concluded that warrants are never required to conduct a cell phone search at the border. *United States v. Williams*, 942 F.3d 1187 (10th Cir. 2019), *cert. denied*, 141 S. Ct. 235 (2020). It upheld a forensic search of a cell phone that was based on reasonable suspicion but expressly "decline[d]" to hold that even reasonable suspicion is required for "searches of personal electronic devices at the border." *Id*. at 1190. The Seventh Circuit relied on good faith to "avoid entirely the thorny issue of the appropriate level of suspicion required" to search digital devices during a customs secondary screening." *United states v. Wanjiku*, 919 F.3d 472, 479 (7th Cir. 2019).

[4] The court ultimately denied the defendant's motion to suppress based on good faith. *Smith*, 2023 WL 3358357, at *11.

phone searches at the border." *Id.* at *8–9. Thus, "phone searches at the border generally require warrants outside exigent circumstances." *Id.* at *11.

The district court rejected the anything-goes approach of the First, Ninth, and Eleventh (and now Fifth) Circuits, which allows the indiscriminate search for digital contraband. The court "doubt[ed] that the government's interest in interdicting so-called 'digital' contraband is genuinely comparable to its historically grounded interest in interdicting physical contraband, since … digital data is rarely stored uniquely on a cell phone such that seizing such a phone with unwanted data really would mean preventing that data from 'entering' the country." *Id* at *9. It acknowledged that "the governmental interest underlying the border search exception is different from that underlying the search-incident-to-arrest exception," in that the former extends to preventing "a wide variety of harmful things from entering the country." *Id.* at *10. But those "things" are different from "data." *Id.* While "that data may contain information relevant to the government's determination as to whether a person should be allowed entry," there is "little heightened interest in blocking entry of the information itself, which is the historical basis for the border search exception." *Id.* Rather, the government's "more general inves-

tigative interest in data about the person or thing entering the country is entirely incidental to the fact of the cell phone being carried over the border, and could just as easily be relied upon to support searches of the person's home, records, or past mail far away from the border." *Id*. (emphasis in original).

Against the relatively weak governmental interest in digital contraband, "a citizen's privacy interests in her cell phone data at the time she presents herself at a U.S. border" are particularly strong. *Id*. at *8. Because "nearly all travelers carry [cell phones] with them, in addition to any physical items, a digital record of more information than could likely be found through a thorough search of that person's home, car, office, mail, and phone, financial and medical records, and more besides." *Id*. "No traveler would reasonably expect to forfeit privacy interests in all this simply by carrying a cell phone when returning home from an international trip." *Id*.

Smith concludes correctly that the warrantless search of a cell phone at the border is unreasonable.

II. The Fourth Amendment prohibits the warrantless search of a cell phone's digital contents at the border.

1. This Court has long recognized that exceptions to the warrant requirement extend only so far as their rationales. *See, e.g., Riley*, 573

U.S. at 385–91; *Arizona v. Gant*, 556 U.S. 332, 351 (2009). The rationales for warrantless border searches of digital data are not present here.

The purpose of the border search exception is not to promote law enforcement or to discover evidence of criminal behavior generally, but to "protect[] this Nation from entrants who may bring anything harmful into [it]." *Montoya de Hernandez*, 473 U.S. at 544; *Ramsey*, 431 U.S. at 606; *United States v. Molina-Isidoro*, 884 F.3d 287, 289, 295 (5th Cir. 2018) (Costa, J., specially concurring) ("[E]very border-search case the Supreme Court has decided involved searches to locate items being smuggled.").

The Court has long distinguished between "[t]he search for and seizure of stolen or forfeited goods, or goods liable to duties," on the one hand, and "a search for and seizure of a man's private books and papers for the purpose ... of using them as evidence against him." *Boyd*, 116 U.S. at 623. "The two things differ *toto coelo*," *id*.—that is, the "whole extent of the heavens," *Molina-Isidoro*, 884 F.3d at 296 (Costa, J., specially concurring). While border agents have long been authorized to search for and seize contraband, "[n]o similar tradition exists for unlimited authority to search and seize items that might help to prove border crimes but are not themselves instrumentalities of the crime." *Id*. at 297. Because "a warrantless search ... must be

limited in scope to that which is justified by the particular purposes served by the exception," *Florida v. Royer*, 460 U.S. 491, 500 (1983) (opinion of White, J.), the border search exception does not authorize the warrantless searches of the digital data on electronic devices.

2. "The ipse dixit that *Riley* 'does not apply to searches at the border,'" which at least the First, Fifth, and Eleventh Circuits (and the Ninth Circuit, in part) expressly conclude, "is 'inadequate' to justify [the circuits'] departures from the structure of [*Riley*'s] reasoning." Note, *The Border Search Muddle*, 132 Harv. L. REV. 2278, 2286 (2019) (quoting *Vergara*, 884 F.3d at 1318 (J. Pryor, J., dissenting)). It relies on an original meaning of the Fourth Amendment that is at best indeterminate and at worst "descriptively false." *Id*. at 2298.

The Court has relied "almost exclusively" on First Congress's Collections Act to articulate the original understanding of the border search exception, making the border categorically different than the interior when it comes to searches. *Id.* at 2289; *see also Ramsey*, 431 U.S. at 616–17 (describing the "historical importance" of the Collections Act as "manifest"). But the historical understanding of this statute allows for competing inferences as to its intended scope. *See Border Search Muddle* at 2290–92 (describing different scholars' historical interpretations of the scope of the Collections Act). For example,

the Act speaks only to ships and vessels and "goods, wares and merchandise," not to a person's "dearest papers" or "'obtaining evidence of crime other than the contraband itself.'" *Id.* at 2292–93 (quoting *United States v. Molina-Isidoro*, 884 F.3d 287, 295 (5th Cir. 2018) (Costa, J., specially concurring)); *id.* at 2295–97. Indeed, the Court acknowledged the limits to warrantless border searches, although without guidance, in *Ramsey*. 431 U.S. at 618 n.13 ("[w]e do not decide whether, and under what circumstances, a border search might be deemed 'unreasonable' because of the particularly offensive manner in which it is carried out").

3. The limits of the border search doctrine must be reconciled with the heightened privacy interests in a traveler's digital data in order to secure "the privacies of life" against "arbitrary power" and to prevent "too permeating police surveillance." *See Carpenter*, 138 S. Ct. at 2214 (cleaned up). Modern digital devices "differ in both a quantitative and a qualitative sense from other objects that" people once traveled with. *Riley*, 573 U.S. at 393. Today's smartphones can store "millions of pages of text, thousands of pictures, or hundreds of videos." *Id.* at 394.

This immense storage capacity "has several interrelated consequences for privacy." *Id.* Digital devices can reveal "nearly every aspect of" a person's life—"from the mundane to the intimate." *Id.* at

395. Not only do these devices collect "in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record," they also can contain data that "date back of the purchase of the phone or even earlier." *Id*. at 394. "Smartphones and laptops contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails." *Kolsuz*, 890 F.3d at 145.

Indiscriminately searching these devices is particularly offense because of the breadth and intimacy of the information they hold, the disclosure of which can cause dignitary and psychological harms. *See* Craig M. Bradley, *Constitutional Protection for Private Papers*, 16 HARV. C.R.-C.L. L. REV. 461, 483 (1981). Searching a digital device "would typically expose to the government far more than the most exhaustive search of a house." *Riley*, 573 U.S. at 396.

4. Modern digital devices are a "pervasive and insistent part of daily life that a proverbial visitor from Mars might conclude that they were an important feature of human anatomy." *Id*. at 385. "[I]t is neither realistic nor reasonable to expect the average traveler to leave his digital devices at home when traveling." *Kolsuz*, 890 F.3d at 145; *see Cotterman*, 709 F.3d at 965. People "compulsively carry cell phones with them all the time." *Carpenter*, 138 S. Ct. at 2218. Cell

phones serve "as digital umbilical cords to what travelers leave behind at home or at work, indispensable travel accessories in their own right, and safety nets to protect against the risks of traveling abroad." *United States v. Saboonchi*, 990 F. Supp. 2d 536, 557–58 (D. Md. 2014).

The number of people crossing the border each year is staggering, and so too are the number of searches of digital data by CBP agents. Customs and Border Patrol reported that officials conducted roughly 37,000 searches of travelers' devices in the 12 months ending in October 2021. Drew Harwell, *Customs Officials Have Copied Americans' Phone Data at Massive Scale*, THE WASHINGTON POST (Sept. 15, 2022). And worse, the government is uploading the data into databases to save for 15 years. *Id.* As many as 3,000 government agents have access to that data. *Id.* No wonder travelers have filed hundreds of complaints with the Department of Homeland Security over suspicionless searches of their digital devices. Charlie Savage & Ron Dixon, *Privacy Complaints Mount Over Phone Searches at U.S. Border Since 2011*, N.Y. TIMES (Dec. 22, 2017).

5. It bears remembering that "the ultimate measure of the constitutionality of a governmental search is 'reasonableness.'" *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 652 (1995). "[T]he reasonableness of a search is determined 'by assessing, on the one hand, the

degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate government interests.'" *United States v. Knights*, 534 U.S. 112, 118–19 (2001) (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)). Applying this traditional formula to the situation here yields a clear outcome: searching a cell phone without a warrant intrudes on personal privacy to an extraordinary and particularly offensive degree and is unnecessary to serve any legitimate governmental interest.

Such searches intrude deeply on an individual's "dignity and privacy interests," *Flores-Montano*, 541 U.S. at 152, for they allow the government to piece together "[t]he sum of an individual's private life," *Riley*, 573 U.S. 394. The indiscriminate rummaging through "the privacies of life" is "particularly offensive" and, given the volume and diversity of private matters to which a customs agents may access, harken back to the reviled writs of assistance of the founding era. *Id.* at 403; *see also Ramsey*, 431 U.S. at 618 n.13.

That some courts have distinguished between manual searches as "routine" and forensic searches as "nonroutine" is a distinction without a difference regarding the government's exercise of arbitrary power to surveil "the privacies of life." The indiscriminate rummaging of a manual search exposes volumes of sensitive data to the roaming eyes of a CBP agent. Indeed, the harm to an individual's privacy that

Riley so thoroughly describes arises out of a manual search. *See* 573 U.S. at 379–81.

The searches of digital data are nothing like the search of a gas tank, "which should be solely a repository for fuel." *Flores-Montano*, 541 U.S. at 154. In short, equating digital searches with predigital searches is like equating a Google search with thumbing through the Yellow Pages (or a trip to the launch pad with a trip to the stables, *Riley*, 573 U.S. at 393). Pointing to child pornography as a kind of digital contraband analogous to its tangible counterparts in print similarly fails to keep the warrantless search tethered to the border exception's purpose. Such reasoning ignores the reality of how digital data is stored and the pervasive use of offsite or cloud storage. *See id.*, at 397–98; *Smith*, 2023 WL 3358357, at *9–10. There are no practical limits that can be employed to cabin the scope of a search to only "digital contraband." *See Riley*, 573 U.S. at 397–98.

On balance, the Fourth Amendment should require the detached scrutiny of a neutral magistrate before allowing customs agents to rummage through the digital contents of a cell phone. Anything less exposes the privacies of life to arbitrary government power and too permeating surveillance.

III. This case is an excellent vehicle for resolving this issue now.

It is time to resolve the question presented. Most circuits have weighed in, and the resulting decisions conflict with each other, as well as this Court's decisions. Only the Court can decide which of the conflicting views of its precedent is correct.

1. The facts of this case would allow the Court to consider different variations of the propriety of cell phone searches and deliver comprehensive guidance on the issue. It is undisputed that, prior to the search of Castillo's phone, the CBP agent had found no evidence that Castillo was involved in a smuggling venture. There was no reasonable suspicion that the phone contained contraband. The stated purpose of the search was to look for evidence of a crime. The agent searched many different applications while Petitioner was effectively under arrest, reviewing multiple forms of communications, before finally opening the photos folder to discover child pornography.

This case affords the Court the opportunity to consider whether it is unreasonable to search digital data at the border without a warrant based on probable cause or whether some lower threshold of suspicion is required; whether the manual-versus-forensic or routine-versus-nonroutine dichotomies are relevant to the search of digital data at the border; and whether any kinds of digital content present different privacy concerns than others.

2. The question presented can only be answered by the Court. Numerous federal court decisions have explored the legal arguments arising from searching cell phones seized at the border and have reached no consensus. These courts openly acknowledge the division. *See, e.g., Cano*, 934 F.3d at 1017–18; *Touset*, 890 F.3d at 1234–35; *Smith*, 2023 WL 3358357, at *7. Additional litigation in the lower courts will not resolve the courts' disagreements over the question presented.

In addition, there is a rich body of academic scholarship exploring the different legal regimes that might govern this issue. *See, e.g.*, *The Border Search Muddle*; Bingzi Hu, *Border Search in the Digital Era: Refashioning the Routine vs. Nonroutine Distinction for Electronic Device Searches*, 49 AM. J. CRIM. 177 (2022) (advocating a heightened standard for all electronic device border searches without designating them as routine or nonroutine); Atanu Das, *Crossing the Line: Department of Homeland Security Border Search of Mobile Device Data Likely Unconstitutional*, 22 U. PA. J. L. & SOC. CHANGE 205 (2019) (concluding that a border search of mobile device data requires a warrant based on probable cause); Eunice Park, *The Elephant in the Room: What is a "Nonroutine" Border Search, Anyway? Digital*

Device Searches Post-Riley, 44 HASTINGS CONST. L.Q. 277 (2017) (concluding all border searches should be subject to a reasonable suspicion standard).

Reexamining the limits on border searches in the context of the modern digital age is vital to knowing the balance between the government's sovereign interests and an individual right to privacy and against unreasonable governmental intrusion. Doing so will yield the answer that there must be a warrant to search the digital contents of a device at the border. *See Riley*, 573 U.S. at 403.

CONCLUSION

FOR THESE REASONS, Petitioner asks this Honorable Court to grant a writ of certiorari.

Respectfully submitted.

MAUREEN SCOTT FRANCO
Federal Public Defender
Western District of Texas
300 Convent Street, Suite 2300
San Antonio, Texas 78205
Tel.: (210) 472-6700
Fax: (210) 472-4454
Kristin_Davidson@fd.org

s/ Kristin L. Davidson
KRISTIN L. DAVIDSON
Assistant Federal Public Defender
Counsel of Record for Petitioner

DATED: October 17, 2023