No. 24-_____

In the Supreme Court of the United States

MARCOS MENDEZ,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

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

PETITION FOR A WRIT OF CERTIORARI

Robert Robertson
Counsel of Record
Marko Duric
ROBERTSON DURIC
One North LaSalle Street
Suite 300
Chicago, IL 60602
(312) 223-8600
robrobertson1@sbcglobal.net
marko@robertsonduric.com

September 9, 2024 *Counsel for Petitioner*

SUPREME COURT PRESS ♦ (888) 958-5705 ♦ BOSTON, MASSACHUSETTS

QUESTIONS PRESENTED

1. Whether the Government may conduct a warrantless search of the electronic contents of a person's cell phone at the border.

2. Whether the Government may conduct a suspicionless search of the electronic contents of a person's cell phone at the border.

LIST OF PROCEEDINGS

United States District Court (N.D. Ill.)

No. 16-cr-163

United States, Plaintiff v. *Marcos Mendez*, Defendant

Judgment: Mar. 8, 2023

United States Court of Appeals, Seventh Circuit

No. 23-1460

United States, Plaintiff-Appellee v.
Marcos Mendez, Defendant-Appellant

Opinion: June 10, 2024

TABLE OF CONTENTS

TABLE OF CONTENTS – Continued

TABLE OF CONTENTS – Continued

Page

APPENDIX TABLE OF CONTENTS

OPINIONS AND ORDERS

OTHER DOCUMENTS

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES – Continued

Page

TABLE OF AUTHORITIES – Continued

Page

CONSTITUTIONAL PROVISIONS

STATUTES

TABLE OF AUTHORITIES – Continued

Page

OTHER AUTHORITIES

PETITION FOR A WRIT OF CERTIORARI

Petitioner Marcos Mendez, by his undersigned counsel, respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Seventh Circuit in this case.

OPINIONS BELOW

The Seventh Circuit's opinion is reported at *United States v. Mendez*, 103 F.4th 1303 and reproduced at App.1a. The judgment of the Northern District of Illinois is included at App.15a. The district court's opinion denying the motion to suppress is reported at *United States v. Mendez*, 2021 WL 3187718 and reproduced at App.18a.

STATEMENT OF JURISDICTION

The Court of Appeals entered judgment on June 10, 2024. This Court has jurisdiction under 28 U.S.C. § 1254(1).

CONSTITUTIONAL PROVISIONS INVOLVED

U.S. Const. amend. IV

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

STATEMENT OF THE CASE

In February 2016, Customs and Border Protection ("CBP") stopped Marcos Mendez and searched his cell phone after he returned home from a trip to Ecuador. App.44a. CPB agents did so on the basis of a "lookout" that instructed CBP agents to interview Mr. Mendez when he returned from his visit abroad. App.44-45a. Lookouts are a daily occurrence. App.45a. They direct CBP agents' attention to certain matters they might need to look into further. *Id.* Here, CBP issued a lookout based on Mr. Mendez's criminal record—a 2011 misdemeanor conviction for endangering the life of a child that followed an arrest for separate child offenses—and a 2014 trip to Mexico during which Mr. Mendez reported that he was kidnapped and all of his electronics were taken. App.44-45a.

At the time Mr. Mendez was stopped and his cell phone searched, CBP had no information that Mr.

Mendez was involved in any criminal activity. App.71a. CBP learned only that Mr. Mendez was returning from a visit to Ecuador with his fiancée. App.84a. Nevertheless, CBP decided to interview Mr. Mendez and conduct a warrantless search of the information stored on his cell phone. CBP made this decision to stop and search Mr. Mendez's cell phone even before he disembarked from his return flight. App.67a.

The stop of Mendez and subsequent cell phone search occurred at around midnight on February 20, 2016, as he returned through O'Hare Airport. App.48-53a. CBP Agent Callison interviewed Mr. Mendez and asked Mr. Mendez to confirm that the items he carried belonged to him. App.50a, 66a. This was done for purposes of prosecution. App.66a. Agent Callison then searched the contents of Mr. Mendez's iPhone, looking through the camera roll as well as files saved in a series of applications called "iSafe." App.53-54a. Agent Callison estimated that it was approximately 45 minutes to one hour from his first interaction with Mr. Mendez to when he stopped looking through Mr. Mendez's phone. App.56a.

After observing child pornography in Mr. Mendez's phone, Agent Callison continued searching the phone with a program called DOMEX. App.59a-61a. The sole purpose of DOMEX was to extract and preserve files for use in a criminal prosecution. App.81a. The DOMEX search lasted approximately two to three hours. *Id.* DOMEX extracted thousands of files from Mr. Mendez's phone, including photographs in the camera roll that were later used to prosecute Mr. Mendez. App.54-56a, 86a. Agent Callison did not seek a warrant prior to using DOMEX, although there were no exigent circumstances and Agent Callison could have placed Mr.

Mendez's phone in airplane mode to prevent remote access. App.79-80a.

CBP allowed Mr. Mendez to clear customs, but retained Mr. Mendez's phone and the data DOMEX extracted. CBP remained with the data extracted through DOMEX even though Mr. Mendez remotely wiped his phone after leaving the airport. App.62-63a.

On March 9, 2016, over two weeks after CBP searched Mr. Mendez's phone, the Government still had not obtained a search warrant. App.97-100a. Nevertheless, Homeland Security analyzed the images extracted from Mr. Mendez's phone with a program called "ExifToolGUI v3.38." *Id*. This allowed agents to review metadata, including creation dates, the type of device that created the file, and the geolocation data showing that photos used in Mr. Mendez's prosecution were taken inside his apartment. App.4a, 98a. All this occurred without a search warrant as well.

On the basis of the evidence obtained as a result of the search of Mr. Mendez's cell phone, the Government charged Mr. Mendez with violating 18 U.S.C. §§ 2251(a), 2252A(a)(1), and 2252A(a)(5)(B). Mr. Mendez moved to suppress on the grounds that the Government's search of his cell phone violated the Fourth Amendment. Mr. Mendez argued that he retained a reasonable expectation of privacy in his cell phone and cited this Court's requirement of a warrant for cell phone searches in *Riley v. California*, 573 U.S. 373 (2014) and *Carpenter v. United States*, 585 U.S. 296 (2018).

At the hearing on Mr. Mendez's motion to suppress, Agent Callison testified as follows:

Q. At the time that you searched Mr. Mendez's cell phone, or just prior to that point, you had no information that he was actively involved in committing a crime, correct?

A. Correct.

Q. You had no information that he was actively involved in child trafficking.

A. Correct.

Q. Had no information he was actively involved in smuggling contraband.

A. Correct.

Q. Including child pornography.

A. Correct . . .

* * *

Q. At the time you conducted what you've described as a manual search of Mr. Mendez's cell phone, you had no social media evidence.

A. Correct. We don't look at any social media.

Q. You had no e-mail evidence.

A. No.

Q. No text message evidence.

A. No.

Q. You had no physical evidence.

A. No.

Q. You found nothing unusual in his luggage.

A. I did not look at his luggage.

Q. Okay. During the course of this entire examination, none of the officers involved found anything unusual in his luggage?

A. Not that I'm aware of.

App.71a-72a.

While Agent Callison claimed that Mr. Mendez was returning from a potential "source country" for child trafficking, he agreed that pretty much any country could be a source of child pornography. App.46a, 70a. And although Agent Callison claimed that Mr. Mendez attempted to deflect attention from the inspection, the basis for this claim was Mr. Mendez's comments to the effect that "He was above being inspected. He was a U.S. citizen. We should just be letting him go." App.50-51a.

In a memorandum opinion and order, the district court denied Mr. Mendez's motion to suppress. The district court relied upon the Seventh Circuit's previous opinion in *United States v. Wanjiku*, which held that the good faith exception to the exclusionary rule applied to the warrantless search of an international traveler's cell phone because there was reasonable suspicion and no court had required more than reasonable suspicion for a border search. App.22a-25a, *citing* 919 F.3d 472, 485 (7th Cir. 2019). Citing *Wanjiku*, the district court disagreed that *Riley* and *Carpenter* were relevant, because "neither case addresse[d] searches at the border where the government's interests are at their zenith." App.25a., *citing* 919 F.3d at 484. The district court went on to find that reasonable suspicion existed based upon Mr. Mendez's: (1) arrest and misdemeanor conviction five years earlier; (2) statement two years earlier that he was kidnapped

and his electronics were taken in Mexico; (3) traveling alone from a "potential source country;" and (4) comments to the effect that Agent Callison should be letting him go. App.29a.

Mr. Mendez later pled guilty in a written plea agreement that reserved his right to appeal the district court's ruling on his motion to suppress. On appeal, the Seventh Circuit did not address the good faith exception or the initial presence of reasonable suspicion. Instead, the Seventh Circuit went much further than its previous opinion in *Wanjiku* and announced a broad rule permitting suspicionless and warrantless searches of electronics at the border. It based its decision on the history supporting the border exception to the Fourth Amendment warrant requirement:

> The longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless 'reasonable' has a history as old as the Fourth Amendment itself. That history leads us to join the uniform view of our sister circuits to hold that searches of electronics at the border—like any other border search—do not require a warrant or probable cause, and that the kind of routine, manual search of the phone initially performed here requires no individualized suspicion.

App.2a.

The Seventh Circuit noted that "Congress, since the beginning of our Government, has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or

a warrant." App.5a, *quoting United States v. Flores-Montano*, 541 U.S. 149, 153 (2004). The Seventh Circuit determined that the initial search of Mr. Mendez's phone was the same type of routine border search, because it lasted "around thirty minutes" and was "practically limited in intrusiveness by the fact that the customs agent . . . [had to] physically scroll through the device, making it less likely for [him] to tap into the revealing nooks and crannies of the phone's metadata, encrypted files, or deleted contents." App.13a.

As for the "extensive forensic searches" that followed the initial "manual" search of Mr. Mendez's phone, the Seventh Circuit held that "[r]outine or otherwise, searches at the border 'never' require a warrant or probable cause." App.7a, *citing United States v. Ramsey*, 431 U.S. 606, 619 (1977). The Seventh Circuit support its conclusion with the fact that "[i]n more than 200 years of border search precedent, neither the Supreme Court nor we have ever found a border search unconstitutional." *Id.*

The Seventh Circuit determined that the high-water mark for privacy protection at the border was set in *United States v. Montoya de Hernandez*, 473 U.S. 531 (1985), which involved the 16-hour detention of a traveler suspected of smuggling drugs in her alimentary canal. App.7a. Because *Montoya de Hernandez* required reasonable suspicion to support a non-routine detention of a suspected drug smuggler, the Seventh Circuit determined that no more than reasonable suspicion is ever required for even the most intrusive, non-routine border searches. *Id.* Suggesting in *dicta* that only a search of someone's person as opposed to devices can be considered non-routine, *id.*, the Seventh Circuit declined to decide whether reasonable suspicion was

required for the non-routine examinations of Mr. Mendez's phone, App.14a. The Seventh Circuit held that even if non-routine searches require reasonable suspicion, the Government obtained reasonable suspicion through its initial search in which Agent Callison scrolled through the phone's contents. *Id.*

The Seventh Circuit dismissed Mr. Mendez's citation to *Riley* and *Carpenter*. As the Seventh Circuit framed it, the issue was whether *Riley* and *Carpenter* "upended" the "long-settled rule exempting border searches from warrant and probable cause requirements." App.7a-8a. The Seventh Circuit answered this question in the negative, again choosing not to apply the reasoning of *Riley* and *Carpenter* on the grounds that these opinions "had nothing to do with the border context." App.8a.

REASONS FOR GRANTING THE PETITION

This case pits constitutionally guaranteed privacy rights in the massive amount of highly personal and sensitive information digitally stored on electronic devices against a rigid, unyielding, and static border search doctrine that wipes away those privacy rights based on where a search occurs. The Circuits have struggled with these competing interests, generating different approaches that seemingly agree on one principle—that the protections provided by the Fourth Amendment as articulated by this Court in *Riley v. California*, 573 U.S. 373 (2014) and *Carpenter v. United States*, 585 U.S. 296 (2018) vanish at the Nation's border. With almost 40 million Americans travelling

abroad every year, and virtually everyone carrying an electronic device, this Court should address these competing concerns, unify the approach to be used by border officials on a daily basis, and update the border search doctrine to deal with our current digital age.

Of particular significance here, the Framers adopted the Fourth Amendment as a response to the arbitrary power of petty British customs officers to search for smuggled goods in private homes without a warrant. The outrage over this practice was in fact one of the complaints that led to the Revolution itself. Two hundred fifty years later, the Courts of Appeals have claimed the mantle of history in granting customs officers the power to arbitrarily search the vast array of personal information contained in a person's cell phone when he or she crosses the border. The Courts of Appeals require nothing—not a warrant, not probable cause, nor even reasonable suspicion—before allowing a border agent to unlock and search through one's entire life laid bare, including all text messages, emails, call histories, photo albums, notes, diary and calendar entries. Millions of Americans would be shocked to learn that they surrender so much of their private lives simply by travelling abroad.

This Court has kept the Fourth Amendment current with our ever-evolving digital world. As technology has advanced, this Court has stressed that the Fourth Amendment protects "that degree of privacy against government that existed when the Fourth Amendment was adopted." *Carpenter*, 585 U.S. at 305, *quoting Kyllo v. United States*, 533 U.S. 27, 34 (2001). The Court has made clear that the "progress of science does not erode Fourth Amendment protections." *Carpenter,* 585 U.S. at 320. This means that the Government

"must generally secure a warrant" before searching the contents of a person's cell phone, *Riley*, 573 U.S. at 386, and likewise "must generally obtain a warrant" before searching cell phone records, *Carpenter*, 585 U.S. at 316. As this Court has explained, searching a person's cell phone is more invasive than "ransacking his house for everything which may incriminate him," for it reveals "a broad array of private information never found in a home in any form—unless the phone is." *Riley*, 573 U.S. at 396, 97.

Yet, the Courts of Appeals have determined that the reasoning of *Riley* and *Carpenter*, and apparently the Fourth Amendment, does not apply at the border. They continue to mechanically apply the border exception, permitting the Government to stop and search all persons and things crossing the border, as if a modern cell phone were no different than a traditional piece of luggage. They have largely dismissed the import of *Riley* and *Carpenter*—that cell phones "differ in both a quantitative and qualitative sense" from other personal effects, *Riley*, 573 U.S. at 393—on the grounds that *Riley* and *Carpenter* were not border search cases.

The Court of Appeals' formulaic approach is inconsistent with this Court's instruction that courts should avoid applying Fourth Amendment exceptions to new technologies in such "mechanical" fashion. *Riley*, 573 U.S. at 386; *see also Carpenter*, 585 U.S. at 318 ("When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents."). This formulaic approach hearkens to a bygone era when Fourth Amendment jurisprudence depended upon the common law of trespass and merely asked whether the Government physically intruded into a constitutionally protected

place. *Carpenter*, 585 U.S. at 304. The Circuits deem electronic device searches reasonable strictly by virtue of taking place at the border. Since *Katz v. United States*, however, the Court has recognized that "the Fourth Amendment protects people, not places." 389 U.S. 347, 351 (1967). Accordingly, "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, 'what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.'" *Carpenter*, 585 U.S. at 310, *quoting Katz*, 389 U.S. at 351-52.

The Circuits' focus on place above all else cannot be reconciled with the proliferation of cell phones and personal computers in the 21st century where travelers carry their entire lives in digital form with them instead of just a few suitcases. Now that border agents routinely search through the large quantities of private information stored on travelers' electronic devices, the Circuits' emphasis of physical place screams the question: What about *Katz, Riley, and Carpenter*? Does a person lose all reasonable expectation of privacy in his or her entire pre-travel life documented in a digital form simply by crossing the border?

This Court has taken only a handful of border search cases. These cases have never involved an invasion of privacy with the depth and breadth of a cell phone search. In the vacuum of guiding authority from this Court, the lower courts have struggled to adequately protect digital privacy at the border. With the privacy rights of millions of Americans hanging in the balance, the Court should grant certiorari to bring its border search precedent into the 21st Century and resolve this vital Fourth Amendment issue.

I. The Court Should Grant Certiorari to Remedy the Circuits' Mechanical Approach

Without guidance from this Court, the Circuits have taken various approaches that all suffer from the same basic flaws illustrated by the Seventh Circuit's opinion below. The Circuits assume history and precedent provide categorical support for suspicionless searches of electronic devices at the border. While acknowledging that these devices differ vastly from traditional personal effects, the Circuits presume these differences don't matter at the border and that customs officers may rummage through the contents of these devices like just another piece of luggage. Customs agents now have the power to search through the troves of personal information on an individual's cell phone for a good reason, a bad reason, or even no reason at all.

A. The Eleventh Circuit Does Not Require Any Suspicion for Any Border Search of Any Electronic Device

The Eleventh Circuit takes the starkest position, ruling that the Fourth Amendment does not require any suspicion for searches of electronic devices at the border, even forensic searches in which the Government relies upon sophisticated computer software. *United States v. Touset*, 890 F.3d 1227 (11th Cir. 2018); *United States v. Vergara*, 884 F.3d 1309 (11th Cir. 2018). Like the other Circuits, the Eleventh claims support for its position in history—namely, the First Congress' passage of the Collection Act, which gave customs officers the authority to conduct warrantless searches of ships entering the country. *Touset*, 890 F.3d at 1232. The Eleventh Circuit equates the forensic

search of a modern cell phone at the border to the customs search of an 18th-century ship; both are reasonable "simply by virtue of the fact that they occur at the border." *Id.* at 1232.

The Eleventh Circuit finds it significant that, while this Court required reasonable suspicion to temporarily detain a suspected drug smuggler in *Montoya de Hernandez*, it "has never required reasonable suspicion for a search of property at the border, however nonroutine and intrusive." *Touset*, 890 F.3d at 1233. In fact, according to the Eleventh Circuit, the Government never needs suspicion for intrusive searches of any property at the border. *Id.* at 1233, 34. As the Eleventh Circuit has put it:

> We see no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property. Just as the United States is entitled to search a fuel tank for drugs, it is entitled to search a flash drive for child pornography. And 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. The same could be said for a recreational vehicle filled with personal effects or a tractor-trailer loaded with boxes of documents. Border agents bear the same responsibility for preventing the importation of contraband in a traveler's possession regardless of advances in technology.

Touset, at 1233.[1]

B. The Ninth Circuit Requires Suspicion Only for Forensic Border Searches of Electronic Devices

The Ninth Circuit employs similar reasoning, but distinguishes between manual and forensic searches of electronic devices. The Ninth Circuit holds that a "manual" search in which a customs officer scrolls through the contents of a person's device does not require any suspicion, while a forensic search requires reasonable suspicion. The Ninth Circuit reasons that a manual search is equivalent to the routine searches and seizures of persons and property customs has historically been allowed to conduct at the border without any suspicion. *United States v. Cotterman*, 709 F.3d 952, 960 (9th Cir. 2013) (initial review of contents of electronic devices akin to suspicionless cursory scan of package in international transit). The Ninth Circuit, however, holds that the substantial privacy interests in electronic devices require the additional modicum of reasonable suspicion for forensic searches. *United States v. Cano*, 934 F.3d 1002, 1013-16 (9th Cir. 2019); *Cotterman*, 709 F.3d at 960-68.

---

[1] In *Vergara*, Eleventh Circuit Judge Jill Pryor wrote a dissenting opinion concluding that *Riley's* reasoning required the Government to obtain a warrant supported by probable cause before it forensically searched the defendant's cell phones. 884 F.3d at 1318 (Pryor, J., dissenting) ("unlike the majority, I do not read *Riley* so narrowly as to prevent its application to cell phone searches in other contexts, including at the border. As the Court went on to explain in *Riley*, '[its holding was] instead that a warrant is generally required before [a cell phone] search . . . '")

C. The First, Third, Fifth, Sixth, and Seventh Circuits Do Not Require Suspicion for "Routine' Border Searches of Electronic Devices

Like the Seventh Circuit, the First and Fifth Circuits have charted a middle path. They agree that the history supporting the border exception permits customs officers to manually scroll through the contents of a traveler's electronic device. But they decline to say whether they will follow the Eleventh or the Ninth Circuit with respect to forensic searches. *United States v. Castillo*, 70 F.4th 894, 897-98 (5th Cir. 2023) ("All we need to decide this case, however, is to adopt the consensus view of our sister circuits and hold that the government can conduct manual cell phone searches at the border without individualized suspicion."); *Alasaad v. Mayorkas*, 988 F.3d 8, 19 (1st Cir. 2021) ("We thus agree with the holdings of the Ninth and Eleventh circuits that basic border searches are routine searches and need not be supported by reasonable suspicion.")

The Third and Sixth Circuits have likewise upheld "routine" searches of electronic devices. *United States v. Stewart*, 729 F.3d 517, 524 (6th Cir. 2013) (upholding non-forensic examination of laptop computers without objection that non-forensic examination was unconstitutional); *United States v. Linarez-Delgado*, 259 F. App'x 506, 508 (3d Cir. 2007) ("Data storage media and electronic equipment, such as films, computer devices, and videotapes, may be inspected and viewed during a reasonable border search."), *citing United States v. Borello*, 766 F.2d 46, 58-59 (2d Cir.1985), *United States v. Ickes*, 393 F.3d 501 (4th Cir.2005).

D. The Fourth, Eighth, and Tenth Circuits Have Employed Reasoning Similar to the Seventh Circuit's Previous *Wanjiku* Decision

The Fourth Circuit holds that forensic border searches and seizures require at least reasonable suspicion, if not a warrant supported by probable cause. *United States v. Nkongho*, 107 F.4th 373, 382 (4th Cir. 2024); *United States v. Aigbekaen*, 943 F.3d 713, 720 (4th Cir. 2019); *United States v. Kolsuz*, 890 F.3d 133, 146 (4th Cir. 2018) ("[a]fter *Riley*, we think it is clear that a forensic search of a digital phone must be treated as a nonroutine border search, requiring some form of individualized suspicion"). Yet, like *Wanjiku*, the Fourth Circuit has chosen to resolve this issue based on the good faith exception to the exclusionary rule announced in *Davis v. United States*, which applies where "binding appellate precedent specifically authorizes a particular police practice." 564 U.S. 229, 241 (2011). And like *Wanjiku*, the Fourth Circuit has fundamentally misapplied this exception. In contrast to *Davis* where there was binding precedent *specifically authorizing* the search, the Fourth Circuit has applied the good faith exception based on the absence of authority around the country proscribing warrantless border searches of electronic devices. *Aigbekaen*, 943 F.3d at 725; *Kolsuz*, 890 F.3d at 147 ("Even as *Riley* has become familiar law, there are no cases requiring more than reasonable suspicion for forensic cell phone searches at the border.").

In a similar vein, the Eighth and Tenth Circuits have upheld forensic searches of electronic devices based on the presence of reasonable suspicion without deciding whether reasonable suspicion is required.

United States v. Williams, 942 F.3d 1187, 1190 (10th Cir. 2019); *United States v. Xiang*, 67 F.4th 895, 901 (8th Cir. 2023) ("But like the Seventh Circuit in *Wanjiku*, we need not decide today whether reasonable suspicion is required for an advanced or forensic border search of electronic devices because we agree with the district court that CBP officers had reasonable suspicion for the forensic search they conducted.")

II. The Court Should Grant Certiorari to Update the Court's Border Search Precedent and Protect That Degree of Privacy That Existed When the Fourth Amendment Was Adopted

In granting the Government the power to conduct suspicionless searches of electronic data at the border, the Circuits have stretched this Court's limited border search precedent and strained the justification for the border exception beyond its breaking point. Neither the historical understanding of the Fourth Amendment, nor the few border search cases decided by this Court, support anything resembling the search of a modern cell phone at the border. History and precedent instead teach that the Framers adopted the Fourth Amendment "to secure 'the privacies of life' against 'arbitrary power,'" *Carpenter*, 585 U.S. at 305, *quoting Boyd v. United States*, 116 U.S. 616, 630 (1886), and would have shuddered to think that security in the intimate details of their private lives depended upon the whims of a customs officer. The Court should grant certiorari to restore the protection against arbitrary government intrusions which the Framers intended.

A. The Historical Understanding of the Fourth Amendment Does Not Support Suscpionless Border Searches of Electronic Devices

History lends little support to the idea that the Government may conduct suspicionless searches of electronic data at the border. The historical support for the border exception is the First Congress' passage of the Collection Act in 1789, granting customs officers the authority to search "any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed." Act of July 31, 1789, ch. 5, § 24, 1 Stat. 29, 43 (repealed 1790). A revised version passed in 1790 allowed customs officers to board vessels "for the purposes of demanding the[ir] manifests . . . and of examining and searching the said ships." Act of Aug. 4, 1790, ch. 35, § 31, 1 Stat. 145, 164 (repealed 1799).

The Collection Act distinguished searches of ships from searches of houses, stories, buildings, or other places, which required customs officers to go before a justice of the peace and obtain a warrant. Indeed, the Framers despised the general writs that gave British customs officers arbitrary discretion to search for smuggled goods wherever the wished. Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH L. REV. 547, 561-67, 580-82 (1999). This British customs practice was described as "'the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law book" in that it placed "the liberty of every man in the hands of every petty officer.'" *Boyd*, 116 U.S. at 625.

The Collection Act likewise said nothing about searching a person's papers. As one commentator has observed, "[t]here is no historical pedigree associated with searches of papers, as opposed to containers capable of concealing physical contraband, at the border." *The Border Search Muddle*, 132 HARV. L. REV. 2278, 2294 (2019). Congress did not authorize the Government to open international letters without a warrant until 1866, and the Department of the Treasury did not assert authority to do so until 1971. *Id.*, *citing United States v. Ramsey*, 431 U.S. 606, 611-12, 612, n.8; *id.* at 626 (Stevens, J., dissenting).

That the framers permitted warrantless searches of ships at the same time they adopted the Fourth Amendment is unsurprising. In the founding era, ships were not equivalent to houses, papers, and effects:

> The absence of legal complaints about general search authority regarding ships is not mysterious. Even during the prerevolutionary struggle with Parliament, American Whigs accepted the legitimacy of extensive government regulation and inspection of shipping. Moreover, no late eighteenth-century lawyer would have imagined that ships were entitled to the same common-law protection due 'houses, papers, and effects.' Ships were not ordinary property at common law, but personalities subject to admiralty law—a branch of civil law . . . In late eighteenth century thought, ships were neither 'houses, papers, and effects [or possessions]' nor 'places.' They were ships."

Davies, *supra*, at 605-06.

Thus, historical support for suspicionless border searches of electronic devices is tenuous at best. Indeed, the widespread reliance on the Collection Act as precedent for these searches is dubious. This is particularly so given that the first iteration of the Act only permitted searches of ships in which collectors had "reason to suspect" items subject to duty. As Justice Ginsburg once noted:

> . . . the particular way the Framers chose to curb the abuses of general warrants . . . was to retain the individualized suspicion requirement contained in the typical general warrant, but to make that requirement meaningful and enforceable, for instance, by raising the required level of individualized suspicion to objective probable cause. So, for example, when the same Congress that proposed the Fourth Amendment authorized duty collectors to search for concealed goods subject to import duties, specific warrants were required for searches on land; but even for searches at sea, where warrants were impractical and thus not required, Congress nonetheless limited officials to searching only those ships and vessels "in which [a collector] *shall have reason to suspect* any goods, wares or merchandise subject to duty shall be concealed."

Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 670-71 (1995) (Ginsburg, J., concurring), *quoting* Act of July 31, 1789, § 24, 1 Stat. 43 (emphasis added).

The chasm between the Collection Act and the modern cell phone is so expansive that it offers little, if any, meaningful support for suspicionless cell phone searches. The search of a person's cell phone cannot

be equated to the search of an 18th-century ship; the search of a cell phone is more invasive than "ransacking his house for everything which may incriminate him." *Riley*, 573 U.S. at 396. If anything can be gleaned from history, it is that the Framers would not have been comfortable granting the power to conduct such a broad general search to petty customs officers acting with neither a warrant nor any suspicion.

B. This Court's Border Search Precedent Does Not Support Suspicionless Border Searches of Electronic Devices

This Court's border search precedent likewise does not support the suspicionless searches of electronic devices at the border. The handful of border search cases the Court has taken up—all involving pre-digital searches—do not address whether a traveler has a reasonable expectation of privacy in anything remotely similar to a cell phone.

The Court first discussed the Government's border authority in *Boyd*, which arose out of a seizure of glass panes at the border. 116 U.S. 616 (1886). Noting that the Collection Act "was passed by the same congress which proposed for adoption the original amendments to the constitution," the Court stated in dicta that "members of that body did not regard searches and seizures of this kind as 'unreasonable,' and they are not embraced within the prohibition of the amendment." *Id.* at 623; *see also Carrol v. United States*, 267 U.S. 132, 150-51 (1925) (noting the border exception as recognized by *Boyd*).

Ninety years later, in *United States v. Ramsey*, the Court addressed the Government's authority to open international mail suspected of containing

contraband. 431 U.S. 606 (1977). Envelopes were opened "only when customs officers h[ad] reason to believe they contain[ed] other than correspondence, while the reading of any correspondence inside the envelopes [was] forbidden." *Id.* The Court upheld this practice under the Government's border authority. Citing *Boyd*, the Court stated that "no extended demonstration" was necessary to establish that "searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border." *Ramsey*, 431 U.S. at 616-17. The Court declared that "[f]rom before the adoption of the Fourth Amendment, border searches have been considered reasonable by the single fact that the person or item in question had entered into our country from outside." *Id.* at 616, 619.

Similarly, in *United States v. Flores-Montano*, the Court upheld the border inspection of a vehicle's gas tank, again citing "the impressive historical pedigree" found in the Collection Act. 541 U.S. 149, 153 (2004). Based on the Government's power to search vehicles at the border, the Court found that the defendant did not have a privacy interest in his gas tank. *Id.* at 154; *see also United States v. Villamonte-Marquez*, 462 U.S. 579, 585 (1983) (finding "impressive historical pedigree" for detention and search of ship with ready access to the sea). Notably, however, the Court left open the possibility that "some searches of property are so destructive as to require a different result." 541 U.S. at 155-56.

The Court's only decision regarding a "non-routine" border search or seizure is its 1985 opinion in *United*

States v. Montoya de Hernandez, which involved the 16-hour detention of a traveler until she voided drug balloons hidden in her alimentary canal. 473 U.S. 531 (1985). The Court framed the question before it as "what level of suspicion would justify a seizure of an incoming traveler for purposes other than a routine border search." *Id.* at 540. The Court answered this question by balancing the government and private interests, admittedly placing its thumb on the scale in favor of the Government. As the Court reasoned, "not only is the expectation of privacy less at the border than in the interior, the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is also struck much more favorably to the Government at the border." *Id.* at 539-40. Based on upon its balancing of the private and Government interests, the Court decided that reasonable suspicion was the appropriate standard for non-routine seizure of persons at the border. *Id.* at 539-41.

The dissent foreshadowed the Fourth Amendment considerations at the core of the subject of this Petition. The dissent criticized the majority opinion for again "converting the Fourth Amendment into a general 'reasonableness' balancing process—a process in which the judicial thumb apparently will be planted firmly on the law enforcement side of the scales." *Id.* at 558 (Brennan, J., *dissenting*). The dissent emphasized that "the Fourth Amendment's Warrant clause is not mere 'dead language' or a bothersome 'inconvenience to be somehow 'weighed' against the claims of police efficiency." *Id.* at 552, *quoting United States v. United States District Court for the Eastern Dist. of Mich.*, 407 U.S. 297, 315 (1972). And the Government

required a warrant for the intrusive seizure involved, the dissent explained, because a traveler does not lose all expectation of privacy at the border:

> The Court further appears to believe that such investigative practices are 'reasonable,' however, on the premise that a traveler's 'expectation of privacy [is] less at the border than in the interior.' This may well be so with respect to routine border inspections, but I do not imagine that decent and law-abiding international travelers have yet reached the point where they 'expect' to be thrown into locked rooms and ordered to excrete into wastebaskets, held incommunicado until they cooperate, or led away in handcuffs to the nearest hospital for exposure to various medical procedures—all on nothing more than the 'reasonable' suspicions of low-ranking enforcement agents. In fact, many people from around the world travel to our borders precisely to escape such unchecked executive investigatory discretion. What a curious first lesson in American liberty awaits them on their arrival.

Montoya de Hernandez, 473 U.S. at 560-61.

The Court has never suggested that any of its border search precedents could be used to justify the search of modern cell phone. In fact, the Court has indicated the opposite. Although *Riley* is not a border search case, its rationale recognizes that a cell phone is not analogous to a traditional physical object that might be found on someone's person. As such, it cannot be treated in a similar manner. 573 U.S. at 393 ("Cell phones differ in both a quantitative and a

qualitative sense from other objects that might be kept on an [individual's] person."). As *Riley* put it, equating a cell phone with an ordinary personal effect "is like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Id.* at 393.

C. Travelling Internationally Does Not Vitiate a Person's Expectation of Privacy in the Digital Contents of a Cell Phone

The Court should grant certiorari to make clear that a person does not surrender the reasonable expectation of privacy in the digital contents of his or her cell phone just by crossing the border. The Circuits' narrow and dispositive focus on physical place fails to account for this Court's command that "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere" and that "'what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.'" *Carpenter*, 585 U.S. at 310, *quoting Katz*, 389 U.S. at 351-52. Missing from the lower courts' analysis is the critical consideration of whether a person passing through customs reasonably expects to retain the privacy of the digital data contained on his or her cell phone. Emblematic is the Seventh Circuit opinion below, which tersely stated "a traveler's expectation of privacy at the border is simply 'less.'" App.6a., *quoting Montoya de Hernandez*, 473 U.S. at 539. The Court should take this opportunity to reiterate "[t]he fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought," *Riley*, 573 U.S. at 403, and that this protection does disappear simply because a person carries a cell phone across the border.

Warrantless searches "are *per se* unreasonable under the Fourth Amendment — subject only to a few specifically established and well-delineated exceptions." *Arizona v. Gant*, 556 U.S. 332, 338 (2009). One of these exceptions is the border exception, which is based on the Government's interest in protecting the integrity of the Nation's border and preventing the entry of contraband. *Montoya de Hernandez*, 473 U.S. at 537-38. That a person generally has a diminished expectation of privacy at the border, however, is not the Alpha and Omega. Where "privacy-related concerns are weighty enough a search may require a warrant, notwithstanding the diminished expectations of privacy of the [individual]." *Riley*, 573 U.S. at 392.

Expecting a routine customs examination of one's person and effects is hardly tantamount to surrendering the privacy of the digital contents of a cell phone. Prior to cell phones, "a search of the person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy." *Id.* at 393. But cell phones "differ in both a quantitative and qualitative sense from other objects that might be kept on an [individual's] person." *Id.* at 393. "[T]he more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate." *Id.* at 395. This includes photographs, picture messages, text messages, Internet browsing history, a calendar, a phone book, notes, prescriptions, bank statements, videos, historic location information, and apps that manage detailed information about all aspects of a person's life. *Id.* at 394-96. Access to this digital record allows the government to

reconstruct "[t]he sum of an individual's private life." *Id.* at 394.

Subjecting the sum of an individual's private life to search cannot be a condition of international travel. *United States v. Smith*, No. 22-CR-352 (JSR), 2023 WL 3358357, at *8 (S.D.N.Y. May 11, 2023) ("Technological and cultural changes now mean that nearly all travelers carry with them, in additional 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. 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."); *Vergara*, 884 F.3d at 1315 (J. Pryor, *dissenting*) (traveler maintains expectation of privacy in cell phone even though privacy interests are diminished at the border). "[M]any people from around the world travel to our borders precisely to escape such unchecked executive investigatory discretion." *Montoya de Hernandez*, 473 U.S. at 558 (Brennan, J., *dissenting*).

Subjecting everyone passing through customs to suspcionless searches of electronic devices may help the Government interdict electronic contraband at the border, but is far too blunt an instrument to justify invading the private lives of millions. It does little to actually interrupt the flow of digital contraband, which criminals can distribute without ever crossing a border. *Vergara*, 884 F.3d at 1317 (J. Pryor, dissenting) ("Unlike physical contraband, electronic contraband is borderless and can be accessed and viewed in the United States without ever having crossed a physical border."). And where, as here, the search of a particular

category of effects is too attenuated from the justifications underlying it, a warrant is required. *Riley*, 573 U.S. at 386, *quoting Gant*, 556 U.S. at 343; *see also Smith*, 2023 WL 3358357, at *8 ("Stopping the cell phone from entering the country would not, in other words, mean stopping the data contained on it from entering the country").

Regardless, however important the Government's interests are at the border, they do not trump a person's expectation of privacy in the electronic details of his or her entire life inside the border. Although suspicionless searches will always serve the Government's interests, the Fourth Amendment warrant requirement is not just simply "'an inconvenience to be somehow 'weighed' against the claims of police efficiency." *Riley*, 573 U.S. at 401. "It is hornbook Fourth Amendment law that '[a] generalized interest in expedient law enforcement cannot, without more, justify a warrantless search.'" *Sec. & Exch. Comm'n v. Jarkesy*, 144 S. Ct. 2117, 2150 (2024) (Gorsuch, J., concurring), *quoting Georgia v. Randolph*, 547 U.S. 103, 115, n. 5, (2006). If the Government intends to invade the privacy of a person's cell phone, the answer is simple—"get a warrant." *Riley*, 573 U.S. at 403.

D. There Is No Reason to Permit a Continuing Warrantless Search of a Person's Cell Phone After Its Seizure at The Border

This case also highlights another troubling and attenuated aspect of border searches of electronic devices—after seizing Mr. Mr. Mendez's phone, the Government continued forensically searching it without a warrant in order to preserve evidence and obtain metadata establishing that photos were taken inside

his apartment. App.4a, 81a, 98a. The Government did so even though it had more than enough time and resources to request a warrant. Although the purpose of these searches was to obtain evidence for Mr. Mendez's prosecution, the Seventh Circuit found that they required no more than reasonable suspicion, which the Government obtained during its initial "manual" search. App.14a. This was error.

"'[W]here a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, . . . reasonableness generally requires the obtaining of a judicial warrant." *Riley*, 573 U.S. at 382, *quoting Vernonia School Dist.*, 515 U.S. at 653. There is no valid reason why, after seizing a cell phone at the border, the Government should be allowed to continue its warrantless search of the phone with sophisticated technology intended for the sole purpose of obtaining evidence for prosecution. This type of search is, in the words of *Riley* and *Gant*, entirely "untether[ed]" form the rationale underlying the border exception. *Riley*, 573 U.S. at 386, *quoting Gant*, 556 U.S. at 343; *see also Aigbekaen*, 943 F.3d at 721 ("the Government may not 'invoke[ ] the border exception on behalf of its generalized interest in law enforcement and combatting crime.").

In sum, the Court should grant certiorari and clarify that a person's reasonable expectation of privacy in the digital contents of a cell phone does not disappear at the border. Before the Government may search through the sum of an individual's private life contained on a cell phone, it must obtain a warrant supported by probable cause. Or at the very least, reasonable suspicion should be required for an initial search and a warrant should be required for subsequent

law-enforcement-related searches. The absence of any real protection for electronic devices at the border is an affront to the Fourth Amendment.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted,

Robert Robertson
Counsel of Record
Marko Duric
ROBERTSON DURIC
One North LaSalle Street
Suite 300
Chicago, IL 60602
(312) 223-8600
robrobertson1@sbcglobal.net
marko@robertsonduric.com

Counsel for Petitioner

September 9, 2024