No.

IN THE

SUPREME COURT OF THE UNITED STATES

HERNANDO JAVIER VERGARA,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

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

PETITION FOR WRIT OF CERTIORARI

Donna Lee Elm
Federal Defender

Adeel M. Bashir*
Assistant Federal Public Defender
Appellate Division
Sup. Ct. Bar. No. 291258
400 N. Tampa Street, Suite 2700
Tampa, FL 33602
Telephone: 813-228-2715
Facsimile: 813-228-2562
E-mail: adeel_bashir@fd.org
*Counsel of Record for Petitioner

QUESTION PRESENTED

In *Riley v. California*, 134 S. Ct. 2473 (2014), this Court explained:

> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans the privacies of life[.] The 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.

Id. at 2494–95 (internal citations and quotation marks omitted). Addressing for the first time how the search incident to arrest exception to the Fourth Amendment's warrant requirement applies to a search of a modern cell phone, *Riley* concluded, "[o]ur answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant." *Id.* at 2495.

This case asks whether *Riley*'s reasoning extends to a search of a citizen's cell phone at the border by means of specialized forensic tools. A divided Eleventh Circuit Panel below held that, "[b]order searches never require probable cause or a warrant," and that *Riley*'s analysis does not apply to border searches, even for forensic searches of cell phones. App. A at 5 (internal quotation marks omitted). The dissent disagreed, concluding that, "[m]y answer to the question of what law enforcement officials must do before forensically searching a cell phone at the border, like the Supreme Court's answer to manually searching a cell phone incident to arrest, 'is accordingly simple—get a warrant.'" App. A at 21 (quoting *Riley*, 134 S. Ct. at 2495). The question presented here is:

> Whether the government may, without a warrant, forensically search a U.S. citizen's cell phone at the border.

TABLE OF CONTENTS

TABLE OF CONTENTS – *cont.*

Section ***Pages(s)***

TABLE OF AUTHORITIES

Cases ***Pages(s)***

TABLE OF AUTHORITIES – *cont.*

Cases ***Pages(s)***

Constitutional Provisions & Statutes

Supreme Court Rules

TABLE OF AUTHORITIES – *cont.*

Federal Agency Authority ***Pages(s)***

Scholarly Articles & Journalistic Sources

TABLE OF AUTHORITIES – *cont.*

Scholarly Articles & Journalistic Sources ***Pages(s)***

TABLE OF AUTHORITIES – *cont.*

Amicus Briefs ***Pages(s)***

Online Sources

PETITION FOR WRIT OF CERTIORARI

Petitioner Hernando Javier Vergara respectfully petitions for a writ of certiorari to review the published decision of the United States Court of Appeals for the Eleventh Circuit, *United States v. Vergara*, 884 F.3d 1309 (11th Cir. 2018).

OPINION BELOW

The United States Court of Appeals for the Eleventh Circuit issued its decision on March 15, 2018. The Eleventh Circuit's divided opinion is attached as Appendix A (App. A).

JURISDICTION

The United States District Court, Middle District of Florida, had jurisdiction over this criminal case under 18 U.S.C. §3231. Under 28 U.S.C. §1291, the Court of Appeals for the Eleventh Circuit had jurisdiction to review the final order of the district court.

Petitioner invokes this Court's jurisdiction under 28 U.S.C. §1254(1). *See* Sup. Ct. R. 14.1(e). This petition is filed timely. *See* Sup. Ct. R. 13.1.

CONSTITUTIONAL PROVISION INVOLVED

The Fourth Amendment states:

> 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 OF THE CASE

This case presents a pressing and recurring question of great national importance following *Riley v. California*, 134 S. Ct. 2473 (2014), about whether the government may, without a warrant, forensically search a citizen's cell phone at the border.

A. Legal Background.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. Amend. IV. "In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement." *Riley*, 134 S. Ct. at 2482.

i. *Riley v. California* and citizens' privacy rights in their cell phones.

In *Riley*, this Court addressed whether the search incident to arrest exception to the Fourth Amendment's warrant requirement applies to a search of a cell phone. *Riley* explained:

> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans the privacies of life[.] The 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. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.

Id. at 2494–95 (internal citations and quotation marks omitted).

Riley makes plain that there is no comparing a search of a cell phone to any physical search. This Court explained that saying a search of all data stored on a cell phone is "materially indistinguishable" from searches of physical items, is "like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Id.* at 2488. *Riley* also makes clear that a search of a cell phone "would typically expose to the government far *more* than the most

exhaustive search of a house," which had traditionally received the highest level of Fourth Amendment protection. *Id.* at 2491 (emphasis in original).

Central to *Riley*'s analysis is its recognition that cell phone data "differ[s] in both a quantitative and a qualitative sense" from other physical items, and that when it comes to cell phones "the possible intrusion on privacy is not physically limited in the same way." *Id.* at 2489.

As *Riley* recognizes, "[o]ne of the most notable distinguishing features of modern cell phones is their immense storage capacity." *Id.* That "storage capacity of cell phones has several interrelated consequences for privacy." *Id.* A "cell phone collects 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." *Id.* "[T]he data on a phone can date back to the purchase of the phone, or even earlier." *Id.* A "cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions[.]" *Id.*

Riley also explains there is "an element of pervasiveness that characterizes cell phones but not physical records." *Id.* at 2490. In the pre-digital world, no one would walk around with hundreds of photos, videos, messages, letters, notes, call records, receipts, bank statements, calendars, directions, maps, magazines, and more. *See id.* But *Riley* acknowledges, "[n]ow it is the person who is not carrying a cell phone, with all that it contains, who is the exception." *Id.*

Riley further recognizes that cell phone data is "qualitatively different" from physical items. *Id.* Data, for instance, can "reveal where a person has been and can reconstruct someone's moments in physical space and determine a person's movements through different websites." *Id.* "Historic location information is a standard feature on many smart phones and can reconstruct

someone's specific movements down to the minute, not only around town but also within a particular building." *Id.* "Mobile application software on a cell phone, or 'apps,' offer a range of tools for managing detailed information about all aspects of a person's life." *Id.*

Riley thus makes clear that a search of a cell phone cannot be compared to a search of a closed container, and that a search for cell phone data cannot be analogized to searching the contents of a container. *See id.* at 2491, 93. After *Riley*, when it comes to privacy, we know that a search of a cell phone is in a category by itself. *See id.* at 2489.

ii. The border search exception to the Fourth Amendment's warrant requirement.

In addition to the search incident to arrest exception at issue in *Riley*, another exception to the Fourth Amendment's warrant requirement applies when searches are conducted at the border. The border search exception, as this Court has explained, is "'like the similar search incident to lawful arrest exception.'" *United States v. Ramsey*, 431 U.S. 606, 621 (1977) (quoting *United States v. Robinson*, 414 U.S. 218, 224 (1973)).

The Court's border search doctrine stems from a trilogy of cases: *Ramsey*, *United States v. Montoya de Hernandez*, 473 U.S. 531 (1985), and *United States v. Flores-Montano*, 541 U.S. 149 (2004). The first case, *Ramsey*, established the principle that officials may conduct "routine" border searches without a warrant or suspicion.

Ramsey involved a customs official's warrantless search of several envelopes (but not the content of the letters themselves) mailed from Thailand to the United States. *Ramsey* upheld the constitutionality of searching those envelopes, explaining that, "searches made at the border, pursuant to the long-standing 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." 431 U.S. at 616.

This Court revisited the border search exception in *Montoya de Hernandez*. There, this Court distinguished between "routine" and "non-routine" border searches and seizures, suggesting that a higher level of process is required for a "non-routine" border search. *See* 473 U.S. at 537–41. *Montoya de Hernandez* involved the detention of a woman flying from Colombia to California, because customs agents suspected she was smuggling cocaine. Agents asked Montoya de Hernandez to take an x-ray to confirm or deny their suspicions, but she claimed she was pregnant and agreed only to take a pregnancy test. Because Montoya de Hernandez refused an x-ray, Customs agents detained her until she produced a monitored bowel movement. After sixteen hours of detention, the agents obtained a court order to conduct a rectal examination, which produced balloons of cocaine. *See id.* at 532–37.

This Court held that the customs agents had reasonable suspicion that Montoya de Hernandez was smuggling drugs in her alimentary canal, and that suspicion was sufficient to justify her temporary detention. *See id.* at 540–41. The Court explained that the reasonable suspicion standard has been applied in situations when "law enforcement officials must make a limited intrusion on less than probable cause." *Id.* at 541. The Court determined that the reasonable suspicion standard "fits well" into situations involving alimentary canal smuggling at the border, because this type of "smuggling gives no external signs, and inspectors will rarely possess probable cause to arrest or search, yet governmental interests in stopping smuggling at the border are high." *Id.*

As in *Ramsey*, the Court in *Montoya de Hernandez* broadly defined the government's interest at the border as "more than merely an investigative law enforcement role[,]" but also as

one in which officials are "protecting this Nation from entrants who may bring anything harmful into this country, whether that be communicable diseases, narcotics, or explosives." *Id.* at 544. The Court adopted the reasonable suspicion standard because an individual's "expectation of privacy is less at the border," and because the "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.

The border search trilogy concludes with *Flores-Montano*. There, the Court addressed the border search exception involving the disassembly of an automobile gasoline tank by customs officials. *See* 541 U.S. at 151. The Court rejected arguments that the defendant had any constitutionally protected privacy interest in his vehicle's gas tank, holding that "the reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person-dignity and privacy interests of the person being searched-simply do not carry over to vehicles." *Id.* at 152. The Court explained that the search of a gas tank was not the kind of "non-routine" or highly intrusive search contemplated by *Montoya de Hernandez*, and "[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.

This Court has not revisited the major contours of the border search doctrine since *Flores-Montano*. This Court also has never addressed how the border search doctrine applies in the unique digital context here: a forensic search of a cell phone.

B. Factual Background and Decisions Below.

i. Facts of the Case.

Hernando Javier Vergara, a United States citizen, arrived at the Port of Tampa, Florida, from a vacation in Cozumel, Mexico. Before his return, U.S. Customs and Border Protection (CBP) had identified Vergara based on his prior conviction for possession of child pornography, placing him on a list of individuals subject to secondary screening. App. A at 2, 9.

Upon Vergara's arrival, CBP Agent Christopher Ragan escorted him to the secondary inspection area. In Vergara's luggage, Ragan found two cell phones, a Samsung cell phone, and an iPhone. *Ibid.* Ragan asked Vergara to turn the Samsung phone on, and then Ragan looked through the phone for about five minutes, including photos and "a couple apps," at first finding nothing of interest. *Ibid.*

Ragan then discovered some videos, one of which depicted topless females he believed were minors. Ragan contacted Special Agent Terri Botterbusch, a criminal investigator with the Department of Homeland Security (DHS). When Botterbusch arrived, she spent a few seconds viewing the video, observing underage, topless females and the logo of a website she knew distributed child pornography. She determined the video was child erotica, meaning it depicted children and was sexual in nature, but it failed to meet the statutory definition of "child pornography." *Id.* at 3, 9–10.

The agents did not have the capability to forensically analyze the phone at the port of entry. Botterbusch therefore seized Vergara's cell phones so "forensic agents" could conduct a full forensic examination using forensic tools. Botterbusch testified that the forensic search involved the extraction of data from the cell phones, and that she believed the forensic search was completed

later that afternoon. The forensic search ultimately revealed over 100 images and videos of child pornography and erotica. *Id.* at 3, 10.

Based on evidence procured from the forensic search, Vergara was arrested and charged with knowingly transporting child pornography, in violation of 18 U.S.C. §2252(a)(1) and (b)(1), and possession of child pornography, in violation of 18 U.S.C. §2252(a)(4)(B) and (b)(2). *Ibid.*

ii. District Court Proceedings.

Vergara moved to suppress the child pornography found on his cell phones. The district court held a suppression hearing, at which Ragan and Botterbusch testified, and later denied Vergara's motion. The district court ruled that the initial manual search did not require reasonable suspicion, and found that, in any event, Agent Ragan had reasonable suspicion to search the applications and settings of the phone. Further, the district court rejected Vergara's argument that *Riley* required the agents to obtain a warrant before conducting the forensic search. It reasoned that *Riley* did not apply to border searches. App. A at 4, 10.

Vergara agreed to a stipulated bench trial, and the district court found him guilty. He was sentenced to 96 months of imprisonment on each count to run concurrently, followed by a lifetime of supervised release. *Ibid.*

iii. The Divided Eleventh Circuit Panel Decision.

On appeal, a divided Eleventh Circuit Panel affirmed the district court's order denying Vergara's motion to suppress.

a. The majority opinion.

Writing for the majority, Judge William Pryor rejected applying *Riley*'s analysis about the significant privacy interests in cell phones to border searches, stating that *Riley* "expressly limited its holding to the search-incident-to-arrest exception." App. A at 6. In the majority's view,

"[b]order searches 'never' require probable cause or a warrant," and nothing in *Riley* disturbs that rule, even for forensic searches of cell phones. *Id.* at 5 (citing *Ramsey*). Accordingly, the majority concluded that the "forensic searches of Vergara's phones required neither a warrant nor probable cause." *Id.* at 6.

b. The dissenting opinion.

In her dissenting opinion, Judge Jill Pryor "disagree[d] with the majority's dismissal of the significant privacy interests implicated in cell phone searches, as articulated by…*Riley*[.]" App. A at 8. The dissent explained:

> Because *Riley* did not involve a border search, I acknowledge that I can, at best, attempt to predict how the Supreme Court would balance the interests here. But my weighing of the government's heightened interest at the border with Vergara's privacy interest in his cell phones leads me to a result different than the majority's. I respectfully dissent because, in my view, a forensic search of a cell phone at the border requires a warrant supported by probable cause.

Id. at 8–9.

Unlike the majority, the dissent embraced *Riley*'s analytical framework by weighing the government's interest in protecting the border against Vergara's privacy interest in his cell phone data. *Id.* at 11.

On the privacy side, the dissent explained that cell phones are "quantitatively" different from "luggage, vehicles, envelopes, and boats that may be searched at the border" "[b]ecause of their 'immense storage capacity.'" *Id.* at 14 (quoting *Riley*, 134 S. Ct. at 2489). The dissent also explained that the "physical realities" that historically have limited border searches do not exist with cell phones. *Id.* at 14.

"Beyond these quantitative differences," the dissent reasoned, "the data cell phones contain is 'also qualitatively different' from the information gleaned by searching luggage, living quarters, and even an individual's person." *Id.* at 15 (quoting *Riley*, 134 S. Ct. at 2490). The

dissent also found that the search here, a forensic examination, was more intrusive than the search in *Riley*. *Id.* at 15. The dissent explained:

> In *Riley*, the officers searched the arrestees' cell phones by viewing videos, reading text messages, and scrolling call logs. Here, Vergara's cell phones were forensically searched. . . . The manual searches in *Riley* were of great concern to the Supreme Court; the forensic examination of cell phones should be of even greater concern given the much more extensive—and more heavily protected from a privacy standpoint—information it may expose.

Id. at 15–16.

On the government's interest side, the dissent acknowledged that the border search exception is rooted in the government's interest in controlling who and what enters the country. *Id.* at 17. The dissent found, however, that those interests "lose force when applied to forensic cell phone searches." *Id.* The dissent explained, "cell phones do not contain the physical contraband that border searches traditionally have prevented from crossing the border, 'whether that be communicable diseases, narcotics, or explosives.'" *Id.* at 17 (quoting *Montoya de Hernandez*). The dissent further explained, "cell phone searches are ill suited to prevent the type of contraband that may be present on a cell phone from entering into the United States." *Id.* at 17. "Unlike physical contraband, electronic contraband is borderless and can be accessed and viewed in the United States without ever having crossed a physical border." *Id*.

The dissent acknowledged that, "forensically searching a cell phone may lead to the discovery of physical contraband." *Id*. Still, the dissent reasoned, "this general law enforcement justification is quite far removed from the purpose originally underlying the border search exception: 'protecting this Nation from entrants who may bring anything harmful into this country.'" *Id.* at 17 (quoting *Montoya de Hernandez*). The dissent thus concluded that, "[e]xcepting forensic cell phone searches from the warrant requirement because those searches

may produce evidence helpful in future criminal investigations would thus 'untether the rule from [its] justifications.'" *Id.* at 17–18 (quoting *Riley*, 134 S. Ct. at 2485).

After discussing the interests at stake, the dissent weighed these interests against one another, concluding that "[r]elative to the importance of the warrant requirement in protecting individual privacy in the type of information a forensic search can reveal—the government's burden in seeking a warrant is minimal." *Id.* at 18. Three practical considerations informed that conclusion.

First, the dissent noted that the same technological advances allowing individuals to carry large caches of sensitive information in pocket-sized devices have also made obtaining a warrant more efficient; in some jurisdictions officers can email warrant requests to judges and receive responses in fewer than 15 minutes. *Id.* at 19 (citing *Riley*, 134 S. Ct. 2493).

Second, the dissent found that forensic searches are themselves an involved process (often conducted off-site with specialized tools), making "the added burden on the government of seeking a warrant slight." *Id.* at 19. "Requiring border officers to seek a warrant before beginning a forensic search, then, would add relatively little time to an already time-intensive process." *Id.*

Third, the dissent concluded, "critically—in the proper circumstances, border officers may still rely on the exigent circumstances exception to conduct a warrantless forensic search." *Id.* at 18 (citing *Riley*, 134 S. Ct. at 2494).

The dissent summarized its position, stating:

> I acknowledge, of course, that because *Riley* concerned a distinct exception to the warrant requirement, it does not compel the outcome I advocate here. The Supreme Court clarified that it was not holding that the information on a cell phone is immune from search. But 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, even when a cell phone is seized incident to arrest. I believe we must look to *Riley* to inform our analysis of Vergara's privacy interest in his cell phones—the very same interests held by the arrestees in *Riley*—to determine whether a warrant is required for a forensic cell phone search even when the search occurs at the border. Due to the extreme intrusion into privacy posed by a forensic cell phone search—well beyond the intrusion posed by a manual search—I would hold that Vergara's privacy interest outweighs the government's interest in conducting such a search, even at the border.

Id. at 20–21 (internal citations, quotation marks, and alterations omitted).

In conclusion, the dissent emphasized the large-scale implications of the majority's holding, stating:

> [A]s the first federal circuit court to determine whether a warrant is required to conduct a forensic search of a cell phone at the border post-*Riley*, the majority's decision likely will have a profound impact on law enforcement practices at our ports of entry and on the individuals subjected to those practices. Last year, customs officers searched more than 30,000 cell phones or other electronic devices of people entering and leaving the United States—nearly a 60 percent increase over the previous year. Meanwhile, for the more than 95 percent of Americans who own cell phones, these devices contain the privacies of life the Fourth Amendment exists to protect. My answer to the question of what law enforcement officials must do before forensically searching a cell phone at the border, like the Supreme Court's answer to manually searching a cell phone incident to arrest, is accordingly simple—get a warrant.

Id. at 21 (internal citations and quotation marks omitted).

REASONS FOR GRANTING THE PETITION

THIS CASE PRESENTS A PRESSING AND RECURRING QUESTION ABOUT WHETHER THE FOURTH AMENDMENT'S WARRANT REQUIREMENT APPLIES TO A FORENSIC SEARCH OF A CITIZEN'S CELL PHONE AT THE BORDER.

In *Riley v. California*, this Court recognized that cell phones are "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." 134 S. Ct. 2473, 2484 (2014). In the four years since *Riley*, cell phone searches at the border have skyrocketed—and so have the complaints about those searches.

This petition asks the Court to answer the pressing and recurring question of whether the government may, without a warrant, forensically search a citizen's cell phone at the border. This issue affects too many Americans for the Court to put off acting. If the Fourth Amendment prohibits forensic searches of cell phones at the border absent exigent circumstances or a warrant, then thousands of citizens have had their Fourth Amendment rights violated, and millions more are at risk of constitutional harm. The problem will only grow with time.

Only this Court can answer this question. This is the right time. This is the right case. The adverse consequences to privacy are too severe for the Court to let the question percolate.

Below, a divided Eleventh Circuit Panel held that border searches never require a warrant, even for a forensic search of a cell phone. That position, however, cannot be the law. This Court's border search precedent does not go even so far as to allow officials to read the contents of a letter. But, by endorsing warrantless forensic cell phone searches, the majority's decision empowers border officials to read conceivably every email and text message a person

ever wrote or received, and to intrude upon a citizen's privacy far *more* than if the officials conducted the most exhaustive search of one's home.

The Founders did not fight a revolution so the government could use the border as a tool to scrutinize the most private aspects of our lives through warrantless forensic searches of our cell phones. The Court should grant the petition and hold that the answer to what law enforcement officials must do before forensically searching a cell phone at the border is simple: "get a warrant." App. A at 21 (Pryor, J., dissenting).

I. The question presented is important, recurring, and affects nearly all Americans.

The Court should grant this petition because, as the dissent stresses, "the majority's decision likely will have a profound impact on law enforcement practices at our ports of entry and on the individuals subjected to those practices." App. A at 21; *see also* Sup. Ct. R. 10(c).[1] Based upon the majority's decision, millions of Americans are subject to having their cell phones forensically searched, without a warrant, in violation of the Fourth Amendment. That Americans will suffer constitutional harm is not theoretical—it is happening today.

Every year millions of Americans cross the border, which includes the border between neighboring countries, every port where a ship docks in this country, and every international airport.[2] Looking just within the Eleventh Circuit, millions of people travel through the busiest

[1] Rule 10(c) provides that one compelling basis for granting a petition for a writ of certiorari is when, as here, "a United States court of appeals has decided an important question of federal law that has not been, but should be, settled by this Court, or has decided an important federal question in a way that conflicts with relevant decisions of this Court."

[2] *See* U.S. Dep't. Trans., Border Crossing/Entry Data, *available at* https://explore.dot.gov/t/BTS/views/BTSBorderCrossingAnnualData/BorderCrossingTableDashboard?:embed=y&:showShareOptions=true&:display_count=no&:showVizHome=no (all websites last accessed on April 21, 2018).

airport in the world—Hartsfield-Jackson International Airport—and the three busiest ports in the world—Port Miami, Port Canaveral, and Port Everglades. *See* Kelly Yamanouchi, *Hartsfield-Jackson Still World's Busiest in Global Ranking*, Atl. J. Const., April 9, 2018; Mary Forgione, *World's Busiest Cruise Ports Are in Florida*, L.A. Times, July 25, 2017.[3]

Meanwhile, over ninety-five percent of Americans own cell phones, which contain "'the privacies of life' the Fourth Amendment exists to protect." App. A at 21 (quoting *Riley*, 134 S. Ct. at 2495); *see also* Pew Research Center, Mobile Technology Fact Sheet, Feb. 5, 2018.[4] Every year, the number of border searches of cell phones continues to surge. *See* Nick Miroff, *U.S. Customs Agents Are Searching More Cellphones—Including Those Belonging to Americans*, Wash. Post, Jan. 5, 2018.[5] "Last year, customs officers searched more than 30,000 cell phones or other electronic devices of people entering and leaving the United States—nearly a 60 percent

---

[3] *Available at* https://www.ajc.com/business/hartsfield-jackson-still-world-busiest-global-ranking/vCRdwcRAlWCjOGFWvoCNCJ/; http://www.latimes.com/travel/cruises/la-tr-cruises-worlds-busiest-cruise-ports-20170721-story.html.

[4] *Available at* http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/. Moreover, nearly half of all U.S. adults own tablet computers and around one-in-five own e-reader devices. *Id.* Over nine-in-ten 18 to 29 year-olds say they live in a household with at least one smartphone, and fifty-one percent of young adults say their home contains three or more such devices. *See* Pew Research Center, 10 Facts About Smartphones as the iPhone turns 10, June 28, 2017, *available at* http://www.pewresearch.org/fact-tank/2017/06/28/10-facts-about-smartphones/.

[5] *Available at* https://www.washingtonpost.com/world/national-security/us-customs-agents-are-searching-more-cellphones--including-those-belonging-to-americans/2018/01/05/0a236202-f247-11e7-b3bf-ab90a706e175_story.html.

increase over the previous year." App. A at 21; *see also* Ron Nixon, *Border Officers Nearly Double Searches of Electronic Devices, U.S. Says*, N.Y. Times, April 11, 2017.[6]

Corresponding with the surge in cell phone border searches is an alarming number of privacy complaints filed by citizens over those searches, particularly forensic searches. *See* Charles Savage, *Privacy Complaints Mount Over Phone Searches at U.S. Border Since 2011*, N.Y. Times, Dec. 22, 2017.[7] "These complaints reveal a range of discriminatory, demeaning, and gratuitously intrusive treatment that travelers have endured at the border, where border agents regularly force them to turn over a digital record of nearly every aspect of their lives without judicial oversight or even individualized suspicion." Press Release, *Knight Institute v. DHS – FOIA Suit on Border Searches of Electronic Devices*.[8] There are even complaints that security officials are searching cell phones of passengers traveling on wholly domestic flights. *See* Alex Johnson, *Suit Demands TSA Explain Phone Searches of Passengers on Domestic Flights*, NBC News, March 13, 2018.[9]

---

[6] *Available at* https://www.nytimes.com/2017/04/11/us/border-customs-officers-electronic-devises-search.html?_r=0.

[7] *Available at* https://www.nytimes.com/interactive/2017/12/22/us/politics/document-KFAI-FOIA-TRIP-Complaints-Border-Electronics.html.

[8] *Available at* https://knightcolumbia.org/content/knight-institute-v-dhs-foia-suit-border-searches-electronic-devices; *see also* KFAI FOIA TRIP Complaints Border Electronics Searches, *available at* https://assets.documentcloud.org/documents/4334752/KFAI-FOIA-TRIP-Complaints-Border-Electronics.pdf.

[9] *Available at* https://www.nbcnews.com/storyline/airplane-mode/suit-demands-tsa-explain-phone-searches-passengers-domestic-flights-n856046.

A civil lawsuit filed by ten citizens highlights these complaints—among the plaintiffs are a military veteran, a journalist, and a NASA engineer. *See Alasaad v. Nielsen*, 1:17-cv-11730 (D. Mass. 2017) (Doc. 7, Amended Complaint, ¶¶14–23). None of these citizens were remotely suspected of committing a crime. Nevertheless, these citizens allege that border officers used the "coercive nature of the secondary inspection environment" to compel them "to unlock their devices or disclose their device password," and "even resort[ed] to physical force in order to conduct electronic device searches." *Id.* ¶48. They argue that, "[a]ll Plaintiffs face a likelihood of future injury" given the frequency with which border officials search cell phones. *Id.* ¶156(a)&(b).

***

The majority's decision in the instant case places millions of Americans at risk of constitutional harm by allowing warrantless forensic searches of their cell phones, in violation of the Fourth Amendment. Unless this Court intervenes, a citizen can do nothing to avoid this harm except to forgo traveling—which is unreasonable; or, to travel without a cell phone—which today is the equivalent of asking a citizen to travel without an essential part of their anatomy. *See Riley*, 134 S. Ct. at 2484.

Simply put, the profound national importance of the question presented warrants this Court's attention. The Court should grant this petition.

II. This is the right time for the Court to intervene, and there is no good reason to delay answering the question presented.

Given the number of Americans that travel with cell phones, the rise in cell phone border searches, and the increasing complaints about those searches, the risk of constitutional harm to

all Americans will continue to grow in time. The Court should grant this petition now and not let this problem manifest any further.

A. There is an urgent need for the Court to intervene because of the adverse consequences to privacy if the majority's decision is allowed to stand.

There is an urgent need for the Court's intervention because of the adverse consequences to privacy if the majority's decision is allowed to stand. As the dissent explains, when it comes to privacy, "the forensic examination of cell phones should be of even greater concern" to the Court than the "manual searches in *Riley*" "given the much more extensive—and more heavily protected from a privacy standpoint—information it may expose." App. A at 16. Consider that one of the leading forensic tools used by law enforcement, Cellebrite, advertises that its search capabilities "[g]o beyond texts, call logs and photos," "bypass passwords, overcome locks and encryption challenges," "extract and preserve public and private data from social media and other cloud-based sources," and "provid[e] an unparalleled amount of forensically sound digital evidence."[10]

This Court's border search doctrine does not go even so far as to allow officials to read the contents of a letter. *See Ramsey*, 431 U.S. at 623.[11] Yet, by endorsing warrantless cell phone searches by means of forensic tools such as Cellebrite, the majority's decision empowers border officials to read every email or text message a person ever wrote or received, including deleted emails and texts. In fact, by endorsing warrantless forensic cell phone searches, the majority's

[10] *See* Features Page, Pro Series, Cellebrite.com, *available at* https://www.cellebrite.com/en/solutions/pro-series/.

[11] "Applicable postal regulations flatly prohibit, under all circumstances, the reading of correspondence absent a search warrant" *Id.*

decision empowers border officials to conduct any of the following searches, despite the absence of probable and a warrant, simply because the search occurs at the border:

- A search of your mobile banking app, containing details of your personal finances;
- A search of your historical GPS locations both domestically and overseas, revealing each place you have visited and when and for how long;
- A search of your social media behavior, both public and private, exposing every social media account you own, every profile picture you looked at, every online post you wrote, and every article you read or "liked";
- A search of all your private photos or videos, detailing when and where you took the photo or video;
- A search of every website you have visited and how long you spent on each;
- A search of every online purchase you made;
- A search of your contact list, identifying every person and organization with whom you have communicated.

By endorsing warrantless forensic cell phone searches, then, the majority's decision radically expands the government's power at the border to search the most private aspects of our lives, well beyond any warrantless intrusion this Court has ever sanctioned. Without this Court's intervention, the majority's decision will significantly compromise Americans' privacy where it matters the most—the chronicles of our lives preserved in perpetuity in our cell phones.

B. There is an urgent need for the Court to intervene because, if allowed to stand, the majority's decision presents serious problems of government abuse of power.

There is also an urgent need for the Court's intervention because, if allowed to stand, the majority's decision raises serious concerns that the government will abuse its power. Take the admission to Congress by the Department of Homeland Security (DHS) that it routinely conducts border searches of cell phones at the request of other government agencies, without specifying

whether that other government agency's request for a search is based on a warrant. *See* DHS Response to Sen. Wyden's Letter dated Feb. 20, 2017.[12] Based upon the majority's decision, nothing is stopping any government agency from using the border as an excuse to examine any citizen's cell phone without obtaining a warrant. The SEC, for instance, could target a corporate CEO to learn details about an upcoming securities issuance, or the FTC could gather details about a potential merger between two corporations.

As another example, suppose the FBI suspects a business executive of fraud, but lacks probable cause to obtain a warrant. Under the majority's rule, the FBI could circumvent the warrant requirement by simply waiting for the CEO to travel through JFK, Dulles, or another of the multitude of America's international airports, and then forensically search the executive's phone. Just as disturbing, the FBI could forensically search the cell phones of the executive's business associates or secretary and read every private conversation the executive had with them.

Allowing the government the power to conduct warrantless forensic cell phone searches could also lead to the unconstitutional targeting of citizens for discriminatory reasons. A border agent, for example, could subject travelers with the name Mohammed to extra security based upon religious bias. *See* Jeff J. Roberts, *Social Media at the Border: Can Agents Ask for Your Facebook Feed?*, Fortune, Feb. 8, 2016 (documenting complaints from Muslim-Americans about CPB agents subjecting their phones and social media accounts to extra scrutiny).[13] Or, a border agent could discriminate against a citizen based upon country of origin, forensically searching

---

[12] *Available at* http://msnbcmedia.msn.com/i/MSNBC/Sections/NEWS/170712-cpb-wyden-letter.pdf.

[13] *Available at* http://fortune.com/2017/02/08/social-media-at-the-border-can-agents-ask-for-your-facebook-feed/.

only the cell phones of Hispanic-Americans traveling from Latin American countries, or the cell phones of Russian-Americans when traveling from Eastern Europe.

What is more, the government could use warrantless forensic cell phone searches at the border for spying on journalists or politicians, undermining additional constitutional rights. For instance, a President could target journalists from left- or right-leaning news organizations to identify sources, or to retaliate for unfriendly news coverage. In addition, a President, whether Republican or Democrat, could order border agents to search the cell phone of an opposing politician to uncover embarrassing information (such as evidence of an extramarital affair), and use that information as ammunition against his opponent.

Most Americans are unaware of the government's extraordinary power to conduct warrantless forensic cell phone searches at the border. *See, e.g.*, Nathan Wessler, *Can Border Agents Search Your Electronic Devices? It's Complicated*, Aclu.org, March 14, 2017.[14] As time goes on and the public becomes increasingly aware of their privacy exposure, there is likely to be a chilling effect on travel, and certainly on traveling with a cell phone. *See, e.g.*, Sara Jodka, *If You Don't Need It, Don't Pack It: Border Searches of Mobile Devices*, Nat'l. L. Rev., March 21, 2018.[15]

This chilling effect is especially burdensome on journalists, lawyers, doctors, and business professionals, who often travel with their cell phones and have an ethical obligation to shield the identities of their sources, clients, and patients and the information they provide. With

[14] *Available at* https://www.aclu.org/blog/privacy-technology/privacy-borders-and-checkpoints/can-border-agents-search-your-electronic.

[15] *Available at* https://www.natlawreview.com/article/if-you-don-t-need-it-don-t-pack-it-border-searches-mobile-devices.

no requirement to obtain a warrant, border agents can engage in fishing expeditions—forensically examining the contents of business travelers' cell phones regardless of any legitimate need to conduct the search—and uncover a host of confidential and proprietary information.

C. Given the clarity of the dispute, further percolation of the question presented is unnecessary.

Not only is there an urgent need for the Court's intervention, there is also no good reason to delay answering this question. The Panel's divided opinion perfectly encapsulates the debate and provides the Court with a complete legal framework needed to resolve the dispute.

On one side of the debate is the majority, which asserts that this Court's border search doctrine sets reasonable suspicion as the highest possible level of process required to perform any search at the border, no matter how intrusive that search may be, including a forensic search of a cell phone. *See* App. A at 5.[16] The majority also flatly denies that *Riley* has any relevance outside the search incident to arrest context. *See id.* at 7.[17]

---

[16] *See also United States v. Molina-Gomez*, 781 F.3d 13, 20 (1st Cir. 2015) (assuming that it was required, reasonable suspicion justified 22-day border search and detention of electronic devices for physical examination); *United States v. Molina-Isidoro*, 884 F.3d 287, 293 (5th Cir. 2018) ("only two of the many federal cases addressing border searches of electronic devices have ever required any level of suspicion"); *United States v. Kolsuz*, 185 F. Supp. 3d 843, 858-59 (E.D. Va. 2016) ("the highest protection available for a border search is reasonable suspicion."); *accord United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013) (holding, pre-*Riley*, that a forensic search of a laptop computer at the border required only reasonable suspicion).

[17] *See also United States v. Escarcega*, 685 F. App'x 354 (5th Cir. 2017) (Rejecting *Riley*'s application to the border search context, stating that, "[w]e apply the law as it stands under holdings of the Supreme Court"); *United States v. Gonzales*, 658 F. App'x 867, 870 (9th Cir. 2016) ("*Riley* did not address border searches, and expressly acknowledged" that phone searches may be justified under other exceptions); *United States v. Ramos*, 190 F. Supp. 3d 992, 1002 (S.D. Cal. 2016) (holding that "it is important to recognize that [*Riley*] did not modify or undercut the paradigmatic border search exception"); *United States v. Saboonchi*, 48 F. Supp. 3d 815, 817-18 (D. Md. 2014); *United States v. Lopez*, 2016 WL 7370030, at *5 (S.D. Cal. Dec. 20, 2016)

On the other side of the debate is the dissent, explaining that:

> 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 . . . I believe we must look to *Riley* to inform our analysis of Vergara's privacy interest in his cell phones—the very same interests held by the arrestees in *Riley*—to determine whether a warrant is required for a forensic cell phone search even when the search occurs at the border.

App. A at 20 (internal citations, quotation marks, and alterations omitted).

Applying *Riley*'s analytical framework, the dissent concludes:

> Due to the extreme intrusion into privacy posed by a forensic cell phone search—well beyond the intrusion posed by a manual search—I would hold that Vergara's privacy interest outweighs the government's interest in conducting such a search, even at the border.

Id. at 20–21.[18]

The dispute between the majority and dissent is clearly drawn. The fundamental disagreement centers over the contours of the border search doctrine and whether *Riley* applies to border searches. Those are disagreements that only this Court can, and should, resolve.

Given the clarity of the dispute, further percolation of the question presented is unnecessary. Additional lower court opinions are unlikely to produce new arguments about the border search doctrine or *Riley* that are not already reflected in the Panel's conflicting opinions.

(holding that *Riley* "does not narrow the limits of a border search"); *United States v. Cano*, 2016 WL 6920449, at *2 (S.D. Cal. Nov. 23, 2016); *Abidor v. Johnson*, No. 10-CV-4059, 2016 WL 3102017, at *6 (E.D.N.Y. June 2, 2016); *United States v. Feiten*, 2016 WL 894452 at *6 (E.D. Mich. 2016) (holding that warrantless border search of electronic device is "utterly consistent" with justifications for border search exception); *United States v. Hernandez*, No. 15-CR-2613-GPC, 2016 WL 471943, at *3 n.2 (S.D. Cal. Feb. 8, 2016); *United States v. Blue*, No. 1-14-CR-244-SCJ, 2015 WL 1519159 at *2 (N.D. Ga. April 1, 2015) (providing that *Riley* "has no direct application to the circumstances" in searching cell phones and computers at the border).

[18] *See also United States v. Caballero*, 178 F. Supp. 3d 1008, 1017 (S.D. Cal. 2016) (stating that, "If this Court were free to decide the question in the first instance, it would hold that the warrantless cell phone search under these circumstances would be unreasonable.").

Indeed, many of the same interest groups that filed as amicus in *Riley*, have filed persuasive amicus briefs in cases across the country advocating in favor of applying *Riley* to cell phone searches at the border.[19] The arguments raised by amici, and the government in reply, mirror the dispute between the majority and dissent below. Further, there are already a number of scholarly articles exploring the doctrinal and policy-related consequences involved with digital searches of electronic devices at the border, which also reflect the dispute between the majority and dissent.[20]

In short, the Panel's conflicting opinions make the question presented ripe for this Court's consideration. Time is of the essence for the Court to provide an answer.

[19] *See, e.g.*, Br. of Amicus Curiae Electronic Freedom Foundation, *et al.*, *United States v. Kolsuz*, No. 16-4687 (4th Cir. *filed* March 20, 2017); Br. of Amicus Curiae The Brennan Center for Justice, Center for Democracy and Technology, *et al.*, *Alasaad v. Nielsen*, No. 17-cv-11730 (D. Mass. *filed* Feb. 2, 2018); Br. of Amicus Curiae The First Amendment Institute at Columbia University and the Reporters Committee for Freedom of the Press, *Alasaad v. Nielsen*, No. 17-cv-11730 (D. Mass. *filed* Feb. 2, 2018); Br. of Amicus Curiae American Civil Liberties Union, *United States v. Molina-Isidoro*, 2017 WL 3720242 (5th Cir. *filed* Aug. 22, 2017).

[20] *See, e.g.*, Thomas M. Miller, *Digital Border Searches after Riley v. California*, 90 Wash. L. Rev. 1943 (2015); *see also* Matthew B. Kugler, *The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study*, 81 U. Chi. L. Rev. 1165 (2014); Orin Kerr, *The Fourth Amendment and the Global Internet*, 67 Stan. L. Rev. 285 (2015).

III. This is the right case for this Court to use for providing a definitive answer to this manifestly important question.

For several reasons, this case is an ideal vehicle for this Court to address the question presented. First, the fact pattern here is comprehensive, straightforward, and undisputed. Accordingly, the question is presented cleanly and boils down to a single issue: Does the Fourth Amendment require law enforcement officials to obtain a warrant before forensically searching a U.S. citizen's cell phone at the border?

Second, as the majority and dissenting opinions reflect, the issue here has been litigated thoroughly, and the arguments have been well preserved at every stage of the litigation. No exception to the exclusionary rule, such as good faith, plain view, or inevitable discovery, applies.[21] The Court's resolution of the question will thus determine the outcome of this case.

Third, the question here specifically involves a forensic cell phone search, as opposed to a manual cell phone search, which makes this a more straightforward case for the Court to resolve.[22] As the dissent explains, a forensic cell phone search is significantly more intrusive than a manual cell phone search, and a forensic search requires more time, expertise, and resources than does a manual search. *See* App. A at 19. At the same time, border officials can email warrant requests to judges and receive responses in less than fifteen minutes, which is less time than it takes to perform a forensic cell phone search. *See id.* at 19 (citing *Riley*, 134 S. Ct. at

[21] *Compare with, Molina-Isidoro*, 884 F.3d at 290–91 (declining to address whether *Riley* applies in the border search context, and, instead, holding that a non-forensic search of Molina's cell phone at the border was supported by probable cause and therefore good faith).

[22] *Accord Birchfield v. N. Dakota*, 136 S. Ct. 2160, 2184 (2016) (concluding that the Fourth Amendment permits law enforcement to perform a breath test during a roadside stop because "the impact of breath tests on privacy is slight;" whereas, the warrant requirement applies to blood tests because "[b]lood tests are significantly more intrusive.").

2493). "Requiring border officers to seek a warrant before beginning a forensic search, then, would add relatively little time to an already time-intensive process." *See id.* at 19.

IV. The majority's decision below is wrong and conflicts with this Court's border search precedent and with *Riley*.

Finally, the Court should grant the petition because the majority's decision conflicts with this Court's border search doctrine and with *Riley*. *See* App. A at 8-21; *see also* Sec. I & n.1, *supra*.

The majority misreads this Court's border precedent, which does not provide that a warrant is "never" required at the border. Even if it did, *Riley* illustrates this Court's willingness to reexamine traditional Fourth Amendment rules as required by new technological realities. *See Riley*, 134 S. Ct. at 2484; *see also Birchfield*, 136 S. Ct. at 2185 ("conclud[ing] that the search-incident-to-arrest doctrine does not justify the warrantless taking of a blood sample"). As this Court has explained, the Court "never relie[s] on stare decisis to justify the continuance of an unconstitutional police practice. And we would be particularly loath to uphold an unconstitutional result in a case that is so easily distinguished from the decisions that arguably compel it." *Arizona v. Gant*, 129 S. Ct. 1710, 1722 (2009).

The majority also misreads *Riley*'s holding as expressly limited to searches incident to arrest. *See* App. A at 19-20 (*Riley*'s statement about "'other case-specific exceptions' "was in response to the government's 'extreme hypotheticals' about the danger of requiring a warrant to search an arrestee's cell phone") (quoting *Riley*, 134 S. Ct. at 2494). Rather, *Riley* explains that the analytical process for determining whether to extend a warrant exception to a search of a cell phone requires, "'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.'" *Riley*, 134 S. Ct. at 2484 (quoting *Wyoming v. Houghton*, 526 U.S. 295, 299 (1999)). The majority refuses to acknowledge *Riley*'s recognition of the unique privacy interests in "[m]odern cell phones, *as a category*." *Id.* at 2489 (emphasis added). That a search occurs at the border does not diminish *Riley*'s recognition of the unique privacy interests in cell phones.

The majority additionally misses that the very purpose of the warrant requirement is to combat the main privacy concern raised by a forensic cell phone search—that a forensic search is open-ended and too easily can amount to a fishing expedition into the most private aspects of our lives. *See Coolidge v. New Hampshire*, 91 S. Ct. 2022, 2038-39 (1971) (internal citations and quotation marks omitted) (providing that, the "specific evil is the general warrant abhorred by the colonists, and the problem is not that of intrusion *per se*, but of a general, exploratory rummaging in a person's belongings.").

At the border, a warrant is an especially valuable protection against "exploratory rummaging" through a cell phone, because a warrant's particularity requirement ensures that a forensic search is tethered to one of the government's border interests. For example, suppose a border agent wishes to forensically search a traveler's cell phone for national security concerns. A warrant's particularity requirement will ensure that the forensic search focuses on identifying terrorist contacts or on markers indicating allegiance to a terrorist organization. In that situation, the government's use of a forensic tool furthers its specific national security interest at the border, but does not allow it to endlessly fish in the cell phone for evidence of any crime generally.

To be sure, DHS claims it has policies to manage border officials' ability to conduct warrantless forensic cell phone searches. *See* U.S. Customs & Border Protection, CBP Directive

No. 3340-049A, Border Search of Electronic Devices (2018).[23] But DHS's policy is fleeting and is no answer to the question in this case. As *Riley* explains, "the Founders did not fight a revolution to gain the right to government agency protocols." *Riley*, 134 S. Ct. at 2491.

Besides, we know from *Riley* that DHS's policy fails to address the Fourth Amendment privacy concerns implicated by a forensic cell phone search. For example, DHS's policy limits border officials from accessing the cloud-content typically available on a cell phone. *See* CBP Directive No. 3340-049A, *supra*, at 4-5. But, *Riley* tells us, this limitation does little to protect privacy because, "[c]ell phone users often may not know whether particular information is stored on the device or in the cloud," and "the same type of data may be stored locally on the device for one user and in the cloud for another." 134 S. Ct. at 2490.

Likewise, DHS policy permits border officials to conduct an "advanced" or forensic search only upon a finding of reasonable suspicion of activity that violates the customs laws or poses a threat to national security. *See* CBP Directive No. 3340-049A, *supra*, at 5. But again, *Riley* tells us that the reasonable suspicion "standard would prove no practical limit at all when it comes to cell phone searches." 134 S. Ct. at 2492.

Indeed, requiring only reasonable suspicion to conduct a forensic cell phone search is an unreasonably low bar to overcome, especially considering the extreme intrusiveness involved with a forensic search. For instance, an agent could allege that the mere fact of a trip to the Cayman Islands or Monte Carlo supports reasonable suspicion of a monetary reporting violation; that a visit to a Middle East country is reasonable suspicion of a national security concern; or that

[23] *Available at* https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf.

a cell phone with an app for sending encrypted messages is reasonable suspicion of both. The point, as *Riley* explains, is that under a reasonable suspicion standard, "[i]t would be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone." *Id.*

***

After *Riley*, courts cannot look at a cell phone as just another piece of luggage or storage container that a citizen carries across the border. As *Riley* explains, cell phones have developed into more than just a technological convenience. "With all they contain and all they may reveal, they hold for many Americans the privacies of life." *Riley*, 134 S. Ct. 2494–95 (internal quotation marks and citations omitted). The fact that technology now allows a citizen to carry the "privacies of life" across the border does not make those privacies any less worthy of protection for which the Founders fought. *See id.* From this Court's analysis in *Riley*, we know that the Fourth Amendment demands even greater protection for cell phones than our homes, and that protection does not disappear simply because a cell phone crosses the border.

The Court should grant the petition in this case, and its answer to the question of what law enforcement officials must do before forensically searching a cell phone at the border, like this Court's answer to manually searching a cell phone incident to arrest in *Riley*, should be accordingly simple—"'get a warrant.'" App. A at 21 (quoting *Riley*, 134 S. Ct. at 2495).

CONCLUSION

This Court has cautioned that new technologies should not be allowed to "erode the privacy guaranteed by the Fourth Amendment." *Kyllo v. United States*, 533 U.S. 27, 34 (2001). Our nation needs the Court to intervene on this important constitutional question, whether the Fourth Amendment permits law enforcement to conduct a warrantless forensic search of a cell phone of a U.S. citizen at the border. For all the foregoing reasons, this petition for a writ of certiorari should be granted.

Respectfully submitted,

Donna Lee Elm
Federal Defender

Adeel M. Bashir*
Assistant Federal Public Defender
Appellate Division
Sup. Ct. Bar. No. 291258
400 N. Tampa Street, Suite 2700
Tampa, FL 33602
Telephone: 813-228-2715
Facsimile: 813-228-2562
E-mail: adeel_bashir@fd.org
*Counsel of Record for Petitioner

APPENDIX A

Appendix A

[PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 16-15059

D.C. Docket No. 8:16-cr-00021-JDW-MAP-1

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

versus

HERNANDO JAVIER VERGARA,

Defendant-Appellant.

Appeal from the United States District Court
for the Middle District of Florida

(March 15, 2018)

Before WILLIAM PRYOR, JILL PRYOR and CLEVENGER,* Circuit Judges.

WILLIAM PRYOR, Circuit Judge:

---

* Honorable Raymond C. Clevenger III, United States Circuit Judge for the Federal Circuit, sitting by designation.

This appeal presents the issue whether warrantless forensic searches of two cell phones at the border violated the Fourth Amendment. U.S. Const. amend IV. Hernando Javier Vergara appeals the denial of his motion to suppress evidence found on two cell phones that he carried on a cruise from Cozumel, Mexico to Tampa, Florida. He argues that the recent decision of the Supreme Court in *Riley v. California*, 134 S. Ct. 2473 (2014)—that the search-incident-to-arrest exception to the warrant requirement does not apply to searches of cell phones—should govern this appeal. But we disagree. The forensic searches of Vergara's cell phones occurred at the border, not as searches incident to arrest, and border searches never require a warrant or probable cause. At most, border searches require reasonable suspicion, but Vergara has not argued that the agents lacked reasonable suspicion to conduct a forensic search of his phones. We affirm.

I. BACKGROUND

Vergara returned to Tampa, Florida, on a cruise ship from Cozumel, Mexico, with three phones: a Samsung phone inside a bag in his luggage, an LG phone, and an iPhone. Christopher Ragan, an officer with Customs and Border Protection, identified Vergara and searched his luggage. When Ragan found the Samsung phone in Vergara's luggage, he asked Vergara to turn the phone on and then looked through the phone for about five minutes. During this search, Ragan found

a video of two topless female minors. After watching a few seconds of that video, Ragan called investigators for the Department of Homeland Security.

After viewing the video and interviewing Vergara, Terri Botterbusch, a special agent with the Department of Homeland Security, decided to have all three phones forensically examined. Agents later returned the iPhone to Vergara's niece after a forensic examination revealed that it did not contain any child pornography.

A forensic examination of the Samsung and LG phones conducted that day revealed more than 100 images and videos, "the production of which involved the use of a minor engaging in sexually explicit conduct and the visual depictions were of such conduct." Neither the earlier manual search nor the forensic examinations damaged the phones. A grand jury later indicted Vergara on two counts: (1) that he "did knowingly transport in and affecting interstate and foreign commerce one or more visual depictions, the production of which involved the use of a minor engaging in sexually explicit conduct and such visual depictions were of such conduct"; and (2) that he "did knowingly possess numerous matters that had been shipped and transported using any means and facility of interstate and foreign commerce, including by computer, which matters contained visual depictions of minors engaging in sexually explicit conduct and the production of which involved the use of minors engaging in sexually explicit conduct." *See* 18 U.S.C. § 2252(a)(1), (b)(1); 18 U.S.C. § 2252(a)(4)(B), (b)(2).

Vergara filed a motion to suppress the evidence obtained from his cell phones. The court held a suppression hearing, at which Ragan and Botterbusch testified, and later denied Vergara's motion. The district court ruled that the initial manual search did not require reasonable suspicion and found that "in any event, . . . Agent Ragan had reasonable suspicion to search the applications and settings of the phone for evidence of child pornography." The district court also rejected Vergara's argument that *Riley v. California*, 134 S. Ct. 2473 (2014), required the agents to obtain a warrant before conducting the forensic search. It reasoned that *Riley* did not apply to border searches. It agreed with the government that "if [Vergara] had entered the country with child pornography images in a notebook, the notebook would have been subject to inspection, and he cannot be allowed to insulate himself from inspection by storing child pornography electronically on his cell phone." And it concluded that, in any event, the search was supported by reasonable suspicion.

At a later bench trial, the district court found Vergara guilty of both counts and later sentenced him to ninety-six months of imprisonment on each count concurrently followed by supervision for life.

II. STANDARD OF REVIEW

"With regard to [a] motion to suppress, we review the district court's factual findings for clear error and its legal conclusions *de novo*." *United States v.*

Newsome, 475 F.3d 1221, 1223 (11th Cir. 2007). We construe all facts "in the light most favorable to the prevailing party below." *Id.* at 1224 (internal quotation marks omitted). And "[t]he individual challenging the search bears the burdens of proof and persuasion." *Id.* (internal quotation marks omitted).

III. DISCUSSION

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 . . . ." U.S. Const. amend. IV. Ordinarily, "where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, reasonableness . . . requires the obtaining of a judicial warrant." *Riley*, 134 S. Ct. at 2482 (alterations adopted) (internal quotation marks omitted). But searches at the border, "from before the adoption of the Fourth Amendment, have been considered to be 'reasonable' by the single fact that the person or item in question had entered into our country from outside." *United States v. Ramsey*, 431 U.S. 606, 619 (1977). Border searches "never" require probable cause or a warrant. *Id.* And we require reasonable suspicion at the border only "for highly intrusive searches of a person's body such as a strip search or an x-ray examination." *United States v. Alfaro-Moncada*, 607 F.3d 720, 729 (11th Cir. 2010).

The forensic searches of Vergara's phones required neither a warrant nor probable cause. "The Supreme Court has consistently held that border searches are not subject to the probable cause and warrant requirements of the Fourth Amendment." *United States v. Vega-Barvo*, 729 F.2d 1341, 1344 (11th Cir. 1984) (citing *Ramsey*, 431 U.S. at 619). Instead, "they are simply subject to that amendment's more amorphous reasonableness standard." *United States v. Villabona-Garnica*, 63 F.3d 1051, 1057 (11th Cir. 1995). 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." *Ramsey*, 431 U.S. at 619. And "[t]here has never been any additional requirement that the reasonableness of a border search depended on the existence of probable cause." *Id.*; *see also United States v. Montoya de Hernandez*, 473 U.S. 531, 537–38 (1985).

Vergara argues that *Riley* required a warrant for both the manual and the forensic searches of his phones, but he challenges only the forensic searches because no evidence from the manual search was admitted as evidence against him. In *Riley*, the Supreme Court addressed the constitutionality of warrantless manual searches of cell phones following the arrest of two defendants in the United States. 134 S. Ct. at 2480–82. And the Supreme Court expressly limited its holding to the search-incident-to-arrest exception. It explained that "even though [that]

exception does not apply to cell phones, other case-specific exceptions may still justify a warrantless search of a particular phone." *Id.* at 2494.

Border searches have long been excepted from warrant and probable cause requirements, and the holding of *Riley* does not change this rule. Vergara points to language from *Riley* about the "consequences for privacy" involved in a search of a cell phone. *Id.* at 2489. But this language does not help him. At the border, the highest standard for a search is reasonable suspicion, *see Vega-Barvo*, 729 F.2d at 1344–45, and Vergara has not challenged the finding of the district court that reasonable suspicion existed for the searches of his phones. So we need not—and do not—address the questions whether reasonable suspicion was required for the searches or whether reasonable suspicion existed.

IV. CONCLUSION

We **AFFIRM** Vergara's judgment of conviction and sentence.

JILL PRYOR, Circuit Judge, dissenting:

In this case we decide for the first time whether a warrantless forensic search of a cell phone at the United States border comports with the Fourth Amendment. To determine whether a law enforcement practice is constitutional, courts must balance its promotion of legitimate government interests against its intrusion on an individual's Fourth Amendment rights. *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985). Here, we weigh the government's interest in conducting warrantless forensic cell phone searches at the border with Hernando Vergara's privacy interest in his cellular devices and the data they contain.

The majority opinion concludes that this balance weighs heavily in the government's favor because the searches occurred at the border. I agree with the majority that the government's interest in protecting the nation is at its peak at the border, but I disagree with the majority's dismissal of the significant privacy interests implicated in cell phone searches, as articulated by the Supreme Court in *Riley v. California*, 134 S. Ct. 2473 (2014). Because *Riley* did not involve a border search, I acknowledge that I can, at best, attempt to predict how the Supreme Court would balance the interests here. But my weighing of the government's heightened interest at the border with Vergara's privacy interest in his cell phones leads me to a result different than the majority's. I respectfully dissent because, in

my view, a forensic search of a cell phone at the border requires a warrant supported by probable cause.

I. BACKGROUND

Vergara, a United States citizen, arrived at the Port of Tampa, Florida, having returned from a vacation in Cozumel, Mexico. Before his return, U.S. Customs and Border Protection ("CBP") had identified Vergara based on his prior conviction for possession of child pornography, placing him on a list of the day's "lookouts." Individuals on the list are subjected to secondary screening at the border, which involves additional questioning and searching.

When Vergara arrived at the port, CBP Agent Christopher Ragan escorted him to the secondary inspection area. In Vergara's luggage, Ragan found two cell phones, a Samsung phone and an iPhone. Vergara also had a third cell phone on his person. Ragan took the Samsung phone and began looking through the photos on it, as well as "a couple apps," finding nothing of interest. Doc. 63 at 12.[1] Ragan then began viewing videos, one of which depicted topless females he believed were minors. Ragan contacted Special Agent Terri Botterbusch, a criminal investigator with the Department of Homeland Security. When Botterbusch arrived, she spent a few seconds viewing the video, observing underage, topless females and the logo of a website that she knew distributed child

[1] All citations in the form "Doc. #" refer to the district court docket entries.

pornography. She determined that the video was child erotica, meaning it depicted children and was sexual in nature, but it failed to meet the statutory definition of child pornography.

The agents "[did not] have the capability to forensic[ally] analyze the phone at the port of entry." Doc. 63 at 23. Botterbusch therefore seized Vergara's cell phones and took them to her office so "forensic agents" could conduct a full forensic examination. *Id.* at 31. The record does not detail the mechanics of the forensic examination, but Botterbusch testified that it involved the "extraction of data" from the cell phones and that she believed it had been completed "that afternoon." *Id.* at 39. The forensic search ultimately revealed more than 100 images and videos of child pornography and erotica stored on Vergara's phones.

Based on evidence procured from the forensic search, Vergara was arrested and charged with knowingly transporting child pornography, in violation of 18 U.S.C. § 2252(a)(1) and (b)(1), and possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2). He filed a motion to suppress the child pornography found on his cell phones; the district court denied the motion. Vergara agreed to a bench trial based on stipulated facts, and the district court found him guilty. He was sentenced to 96 months of imprisonment. Vergara appealed.

II. DISCUSSION

The Fourth Amendment establishes "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ." U.S. Const. amend IV. "As the text makes clear, the ultimate touchstone of the Fourth Amendment is reasonableness." *Riley*, 134 S. Ct. at 2482 (internal quotation marks omitted). In general, reasonableness requires the government to obtain a judicial warrant supported by probable cause prior to conducting a search. *Id.* To "determine whether to exempt a given type of search from the warrant requirement," courts weigh the degree to which the practice promotes "legitimate governmental interests" against "the degree to which it intrudes upon an individual's privacy." *Id.* at 2484. This case requires us to balance the government's interest in protecting the integrity of the border against Vergara's privacy interest in the data extracted from his cell phones.

Congress has granted the Executive Branch the "plenary authority to conduct routine searches . . . at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country." *Montoya de Hernandez*, 473 U.S. at 537. This exception to the warrant requirement "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." *United States v. Ramsey*, 431

U.S. 606, 620 (1977). Because of the "paramount interest in protecting . . . its territorial integrity," the government's interest at the border is "at its zenith." *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004).

Given the government's heightened interest, the Supreme Court has held, for example, that at the border mail may be opened without a warrant, vehicles may be stopped without individualized suspicion, and boats may be boarded "with no suspicion whatever." *Montoya de Hernandez*, 473 U.S. at 538; *see also Flores-Montano*, 541 U.S. at 155 (holding that at the border a vehicle's gas tank may be disassembled and searched without any suspicion). Consistently with the Supreme Court's cases involving routine border searches, we have held that living quarters on a ship may be searched at the border absent any suspicion. *United States v. Alfaro-Moncada*, 607 F.3d 720, 732 (11th Cir. 2010). Such searches "are reasonable simply by virtue of the fact that they occur at the border." *Flores-Montano*, 541 U.S. at 152-53 (internal quotation marks omitted).

But the government's authority at the border is not without limits. In *Montoya de Hernandez*, for example, the Supreme Court held that the prolonged detention of a woman who was suspected of smuggling narcotics within her alimentary canal was "beyond the scope of a routine customs search" and thus required some level of suspicion. *Montoya de Hernandez*, 473 U.S. at 541. Although the Court expressed "no view" on the level of suspicion required for

"nonroutine border searches," *id.* at 541 n.4, our circuit has held that "highly intrusive searches of a person's body such as a strip search or an x-ray examination" require reasonable suspicion, *Alfaro-Moncada*, 607 F.3d at 729.

Neither the Supreme Court nor any federal circuit court has determined the level of suspicion required to justify the forensic search of a cell phone at the border.[2] But in *Riley*, the Supreme Court suggested an answer by holding that probable cause and a warrant are required to manually search a cell phone following a lawful arrest. 134 S. Ct. at 2485. The Supreme Court described in *Riley* the significant privacy interests that individuals hold in the contents of their cell phones. And, as I will explain, the privacy interests implicated in *forensic* searches are even greater than those involved in the manual searches at issue in *Riley*. In view of those interests, I would hold that a forensic search of a cell phone at the border requires a warrant supported by probable cause.[3]

As the Supreme Court made clear in *Riley*, cell phones are fundamentally different from any object traditionally subject to government search at the border.

---

[2] In *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013), the Ninth Circuit determined that a forensic search of a laptop computer at the border required reasonable suspicion. That case, however, was decided prior to the Supreme Court's decision in *Riley*, which, as I explain below, suggests that probable cause and a warrant might be required for a forensic search of a cell phone even at the border.

[3] As the majority notes, because the evidence leading to Vergara's conviction stemmed only from the forensic search, we need not consider the level of suspicion required to support the initial, manual search of the cell phones.

See id. at 2489 (explaining that "[t]he term 'cell phone' is itself misleading," given that such devices "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.") Because of their "immense storage capacity," these devices "differ in a quantitative . . . sense" from the luggage, vehicles, envelopes, and boats that may be searched at the border without suspicion. *Id.* Unlike those physical objects, cell phones have the capacity to store "millions of pages of text, thousands of pictures, or hundreds of videos." *Id.*

Before cell phones, border searches were limited by "physical realities" that ensured any search would impose a relatively narrow intrusion on privacy. *See id.* Individuals could not carry across the border all the mail they had received, pictures they had taken, and books they had read. *See id*. When it comes to cell phone searches, though, these "physical realities" no longer exist. *Id.* And, as the Court predicted in *Riley*, the "gulf between physical practicability and digital capacity will only continue to widen." *Id.*[4]

Beyond these quantitative differences, the data cell phones contain is "also qualitatively different" from the information gleaned by searching luggage, living

[4] At the time *Riley* was decided, the "top-selling smart phone" had a standard capacity of 16 gigabytes—the equivalent of millions of physical pages of text. *Riley*, 134 S. Ct. at 2489. Today, the standard storage capacity of that smart phone has doubled to 32 gigabytes. *See* Tech Specs for Apple iPhone 7, https://www.apple.com/iphone-7/specs/ (last visited Mar. 13, 2018).

quarters, and even an individual's person. *Id*. at 2490. A cell phone's internet search history can "reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD." *Id*. Cell phone data also may "reveal where a person has been." *Id.* And cell phone applications as well as data offer a range of information on such private and personal topics as addiction, religious practices, pregnancy, personal finances, and romance. *See id.*

The Supreme Court recognized in *Riley* that given the vast amounts of personal information contained on a cell phone, a cell phone search "typically expose[s] to the government far *more* than the most exhaustive search of a house," which has historically received the Fourth Amendment's most stringent protections. *Id*. at 2491. Indeed, a cell phone "not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is." *Id.*

Although the government's interest at the border is undoubtedly greater than it was in searching the arrestees in *Riley*, Vergara's privacy interests are greater here, too. In *Riley*, the officers searched the arrestees' cell phones by viewing videos, reading text messages, and scrolling call logs. Here, Vergara's cell phones were forensically searched. Although the record does not reveal what that

examination entailed, generally, forensic searches are "experts' work," performed "by a trained analyst at a government forensics laboratory." Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 537 (2005). These examinations reveal "a wealth of information about how the [device] and its contents have been used." *Id.* at 542. Significantly, forensic searches are "capable of unlocking password-protected files, restoring deleted material, and retrieving images viewed on web sites." *Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013). The manual searches in *Riley* were of great concern to the Supreme Court; the forensic examination of cell phones should be of even greater concern given the much more extensive—and more heavily protected from a privacy standpoint—information it may expose.

Of course, the border search exception to the warrant requirement "rests not only on the heightened government interests . . . but also on [travelers'] reduced privacy interests" at the border. *Riley*, 134 S. Ct. at 2488; *see Montoya de Hernandez*, 473 U.S. at 539 ("[T]he expectation of privacy is less at the border than in the interior."). But a "diminished privacy interest[] does not mean that the Fourth Amendment falls out of the picture entirely." *Riley*, 134 S. Ct. at 2488. Instead, when the "privacy-related concerns are weighty enough," as they are in a forensic search of a cell phone, the search may require a warrant, "notwithstanding the diminished expectations of privacy." *Id.* (internal quotation marks omitted).

Applying the Supreme Court's reasoning in *Riley*, the rationales underlying the border search exception lose force when applied to forensic cell phone searches. The border search exception is rooted in the government's interest in controlling "who and what may enter the country." *Ramsey*, 431 U.S. at 620. But cell phones do not contain the physical contraband that border searches traditionally have prevented from crossing the border, "whether that be communicable diseases, narcotics, or explosives." *Montoya de Hernandez*, 473 U.S. at 544. And cell phone searches are ill suited to prevent the type of contraband that may be present on a cell phone from entering into the United States. Unlike physical contraband, electronic contraband is borderless and can be accessed and viewed in the United States without ever having crossed a physical border.

To be sure, forensically searching a cell phone may lead to the discovery of physical contraband. A drug smuggler's deleted text messages, for example, may reveal the location of drugs inside the border. But this general law enforcement justification is quite far removed from the purpose originally underlying the border search exception: "protecting this Nation from entrants who may bring anything harmful into this country." *Id.* Excepting forensic cell phone searches from the warrant requirement because those searches may produce evidence helpful in

future criminal investigations would thus "untether the rule from [its] justifications." *Riley*, 134 S. Ct. at 2485 (internal quotation marks omitted).

The government argues that requiring probable cause and a warrant before conducting a forensic search would allow "terrorists, spies, [and] smugglers" to cross the border knowing their "devices will be immune from random, unpredictable, and suspicionless searches." Appellee's Br. at 26. Certainly, cell phones may contain information about past, present, and future criminal activity. But obtaining a warrant before extracting data from a cell phone is "not merely an inconvenience to be . . . weighed against the claims of police efficiency"; instead, it is a process essential to the "machinery of our government." *Riley*, 134 S. Ct. at 2493 (internal quotation marks omitted). The warrant requirement prevents the government from boundlessly intruding on individuals' privacy "on the mere chance that desired evidence might be obtained." *Montoya de Hernandez*, 473 U.S. at 540 n.3 (internal quotation marks omitted). And—critically—in the proper circumstances, border officers may still rely on the exigent circumstances exception to conduct a warrantless forensic search. *See Riley*, 134 S. Ct. at 2494.

Relative to the importance of the warrant requirement in protecting individual privacy in the type of information a forensic search can reveal—the government's burden in seeking a warrant is minimal. Indeed, the same technological advances that have enabled "smart" cellular devices have made the

process of obtaining a warrant more efficient. The Federal Rules of Criminal Procedure allow judges to issue warrants "by reliable electronic means." Fed. R. Crim. P. 4.1(b)(6)(C). As the Supreme Court noted in *Riley*, in some jurisdictions officers can e-mail warrant requests to judges and receive responses in fewer than 15 minutes. 134 S. Ct. at 2493.

Forensic searches are themselves an involved process, making the added burden on the government of seeking a warrant slight. In general, forensic examinations require "analysts [to] sift through the mountain of data in a hard drive and locate specific types or pieces of data." Kerr, *Searches and Seizures in a Digital World*, *supra* page 9, at 538. This process involves "a range of software programs to aid the search, [and] can take many days or even weeks to complete." *Id.* In this case, Agent Botterbusch had to transport Vergara's phones to her office where special forensic agents had to conduct the forensic search. Requiring border officers to seek a warrant before beginning a forensic search, then, would add relatively little time to an already time-intensive process.

I disagree with the majority that *Riley* is irrelevant to the forensic searches of Vergara's cell phones because the Supreme Court "expressly limited its holding to the search-incident-to-arrest exception." Maj. Op. at 7. The majority relies on the Supreme Court's statement that "other case-specific exceptions may still justify a warrantless search of a particular phone." *Riley*, 134 S. Ct. at 2494. But that

statement was in response to the government's "extreme hypotheticals" about the danger of requiring a warrant to search an arrestee's cell phone, for example, when "a suspect [is] texting an accomplice who . . . is preparing to detonate a bomb." *Id*. To allay the government's concerns, the Supreme Court clarified that exceptions to the warrant requirement, like the exigent circumstances exception, would still be available in the proper circumstances. *Id.*

I acknowledge, of course, that because *Riley* concerned a distinct exception to the warrant requirement, it does not compel the outcome I advocate here. The Supreme Court clarified that it was not holding "that the information on a cell phone is immune from search." *Id*. at 2493. But 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, *even when* a cell phone is seized incident to arrest." *Id.* (emphasis added). I believe we must look to *Riley* to inform our analysis of Vergara's privacy interest in his cell phones—the very same interests held by the arrestees in *Riley*—to determine whether a warrant is required for a forensic cell phone search *even when* the search occurs at the border. Due to the extreme intrusion into privacy posed by a forensic cell phone search—well beyond the intrusion posed by a manual

search—I would hold that Vergara's privacy interest outweighs the government's interest in conducting such a search, even at the border.

I note finally that, as the first federal circuit court to determine whether a warrant is required to conduct a forensic search of a cell phone at the border post-*Riley*, the majority's decision likely will have a profound impact on law enforcement practices at our ports of entry and on the individuals subjected to those practices. Last year, customs officers searched more than 30,000 cell phones or other electronic devices of people entering and leaving the United States—nearly a 60 percent increase over the previous year.[5] Meanwhile, for the more than 95 percent of Americans who own cell phones,[6] these devices contain "the privacies of life" the Fourth Amendment exists to protect. *Riley*, 134 S. Ct. 2495 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)). My answer to the question of what law enforcement officials must do before forensically searching a cell phone at the border, like the Supreme Court's answer to manually searching a cell phone incident to arrest, "is accordingly simple—get a warrant." *Id.*

---

[5] *CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics*, U.S. Customs and Border Protection (Jan. 5, 2018), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and.

[6] Pew Research Center, Mobile Fact Sheet (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/mobile/.