No. 19-1221

In the Supreme Court of the United States

DERRICK LUCIUS WILLIAMS, JR.,

PETITIONER

v.

UNITED STATES OF AMERICA,

RESPONDENT

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

BRIEF FOR RESPONDENT

Matt Clarkston
Counsel of Record
UNIVERSITY OF CALIFORNIA, BERKELEY, SCHOOL OF LAW
225 Bancroft Way
Berkeley, CA 94720

QUESTION PRESENTED

What is the appropriate legal standard under the Fourth Amendment for government agents to conduct a warrantless forensic search of a digital device at the border?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Constitutional Provisions

INTRODUCTION

Each day, 1.1 million individuals pass through America's border and ports of entry. U.S. Customs and Border Protection, *Snapshot*: *A Summary of CBP Facts and Figures* (2020) (*hereinafter* "CBP, *Snapshot*"). Border officials like Agents Kyle Allen and Christopher McGuckin face a daunting challenge: screening those 1.1 million people and their effects to enforce our customs and immigration laws and protect our nation's security.

In pursuit of this mission, Agent Allen issued a "lookout" alert for petitioner Derrick Williams after learning of petitioner's arrest in Germany for weapons violations. When petitioner later arrived at Denver International Airport on a flight from Paris, it triggered the alert, prompting officials to direct petitioner to a secondary inspection and interview location.

As Agent Allen questioned petitioner about his travels abroad, computer forensic agents seized his laptop and phone. Agent McGuckin began a forensic search of the contents of petitioner's laptop – a search that ultimately turned up thousands of images and videos of child pornography.

However, had petitioner instead flown into an airport in a different part of the country, the search that uncovered his collection of child pornography might never have occurred.

Circuit courts around the country have reached a number of conflicting conclusions on when border agents can conduct such forensic digital searches in accordance with the Fourth Amendment. The Ninth Circuit only permits forensic border searches when agents have reason to suspect that the search will reveal digital contraband. The Fourth Circuit goes slightly further, allowing searches for evidence of crimes in addition to contraband itself, but only when agents reasonably suspect that the crime is "transnational." In the instant case, the Tenth Circuit affirmed the denial of petitioner's motion to suppress, holding that reasonable suspicion of *any* criminal activity justifies a forensic search. And in the Eleventh Circuit, border agents may

conduct forensic digital searches without any particular suspicion. The ability of officials to protect the nation's border should not depend on geographic chance; this case presents the opportunity to clarify the issue of when border agents may conduct forensic digital searches.

This Court has long recognized that the Fourth Amendment affords border officials significant latitude to discharge their important mission. Individuals have a diminished expectation of privacy at the border, and the government's interest in regulating who and what enter the country is at its peak at the border. Balancing those interests, this Court has never required officials to possess reasonable suspicion for a search at the border.

Accordingly, the Eleventh Circuit's standard correctly applies this Court's precedents: forensic border searches are reasonable without any particularized suspicion. This Court has recognized the significant privacy interest individuals have in their digital devices, but forensic digital searches are also vital to the government's interests at the border. Thus, this heightened privacy interest still does not overcome the fact that at the border, the balance of individual and government interests simply tilts "much more favorably to the Government." *United States v. Montoya de Hernandez*, 473 U.S. 531, 540 (1985).

However, if this Court determines that forensic searches must be supported by reasonable suspicion, it should affirm the holding of the panel below that suspicion of *any* criminal activity justifies the search. The alternative reasonable suspicion standards proffered by the Ninth and Fourth Circuits have no foundation in precedent, misunderstand and misapply the purposes underlying border search authority, and ignore practical realities.

As digital devices take on an ever-increasing role in the world, the challenge that border agents face only grows. This Court can ensure that border agents have the tools needed to meet that challenge.

STATEMENT OF THE CASE

I. Factual Background

Homeland Security Special Agent Kyle Allen first became aware of petitioner Derrick Williams in August 2015. R. at 14-15. Allen received a letter from the FBI stating that German authorities had arrested petitioner for violating its weapons laws. R. at 15. Because of the weapons violations, German authorities forced petitioner to leave the country. R. at 15. The investigation by German authorities revealed that petitioner had previously been deported from Germany in 2011 due to an expired visa. R. at 15.

Upon receiving this letter, Agent Allen further investigated petitioner. R. at 16. Agent Allen discovered petitioner's extensive European travel history, as well as his criminal history, which included convictions for trespass, fraud, and escape. R. at 16. The latter conviction stemmed from petitioner skipping parole by fleeing to Germany prior to his 2011 deportation. R. at 16.

In November 2015, in response to a series of major terrorist attacks in France with suspects linked to several locations in Europe, Agent Allen's supervisors requested him to review his open files to determine if any persons might be "of interest." R. at 16. As a result, though Agent Allen had no specific link of petitioner to the attack, he placed a "lookout" alert in the U.S. Customs and Border Protection database. R. at 16-17.

Six days after it was placed, petitioner triggered the "lookout" alert when he boarded a flight from Paris bound for Denver. R. at 17. Upon arrival at Denver International Airport, petitioner was directed to a secondary inspection area and interview room. R. at 18.

There, Agent Allen conducted a thirty-minute interview with petitioner. R. at 18. During this time, computer forensic agents began examining petitioner's laptop and phone. R. at 18. In the interview, Agent Allen questioned petitioner about his months-long travels abroad, though at

times, petitioner could not remember details of his purported activities. R. at 18-19. Petitioner omitted Germany from the list of countries visited on his customs form, though Agent Allen knew he had been in the country given his German arrest. R. at 17-18. When Agent Allen asked petitioner directly about being in Germany, petitioner was evasive. R. 20-21.

In the meantime, forensic agents continued to work on petitioner's devices. R. at 19. Petitioner refused to give his passwords to Agent Allen, who informed petitioner that because the searches would therefore take longer, he could leave, and the devices would be mailed to him later. R. at 20-21. Petitioner then left the airport. R. at 21.

The next day, computer forensic agent Christopher McGuckin began initially examining the devices, a process that would take several days. R. at 21-22. McGuckin began by making a complete copy of the laptop hard drive to avoid damaging any contents of the original. R. at 22. He then used a forensic analysis program called EnCase to explore the copied contents. R. at 22-23.

A folder titled "Issue 15 Little Duchess" quickly drew McGuckin's attention. R. at 23. McGuckin opened the folder and soon discovered child pornography. R. at 23. He stopped his search and alerted Agent Allen, who applied for and obtained a search warrant. R. at 23.

Pursuant to the warrant, McGuckin conducted an exhaustive search of petitioner's laptop that ultimately turned up thousands of images and videos of child pornography. R. at 24. Petitioner's phone was also searched, but no child pornography was discovered. R. at 24.

Petitioner was then indicted and arrested on charges of transporting and possessing child pornography. R. at 24. Petitioner moved to suppress the evidence of the child pornography as the product of an unreasonable search under the Fourth Amendment. R. at 24. The district court declined to weigh in on whether the forensic search required reasonable suspicion or no

particularized suspicion. R. at 30-31. Rather, it found that agents had reasonable suspicion that petitioner had violated 18 U.S.C. § 1001, prohibiting false statements to federal officers, by omitting Germany from the list of countries he had visited. R. at 34. Further, it concluded that petitioner's evasive answers when questioned about being in Germany created reasonable suspicion of other offenses, such as violation of customs laws. R. at 34-35. Because agents could reasonably suspect that petitioner's laptop would contain evidence relevant to such offenses, the forensic search was not unreasonable, and the court denied the motion to suppress. R. at 35, 37.

II. Legal Background

Circuit courts have reached a number of differing conclusions as to what standard of suspicion is required for a forensic digital search at the border. All agree that searches may be conducted without a warrant, pursuant to the border search exception to the warrant requirement. Three of them, including the panel below, have applied some form of reasonable suspicion, though they diverge as to what form that suspicion must take. Another, the Eleventh Circuit, has held that forensic searches are justified without any particularized suspicion.

The Fourth Amendment protects individuals against "unreasonable searches and seizures." U.S. Const. amend. IV. While in many cases this means that officials must have a warrant supported by probable cause to search, warrantless searches are nonetheless permissible when conducted pursuant to one of a number of well-established exceptions to the warrant requirement. *Katz v. United States*, 389 U.S. 347, 357 (1967). Some searches pursuant to an exception require officials to have some degree of particularized suspicion about the target of the search to be reasonable under the Fourth Amendment; others require no particularized suspicion. *See, e.g., Carroll v. United States*, 267 U.S. 132, 154 (1925) (requiring probable cause for searches under the automobile exception); *Chimel v. California*, 395 U.S. 752, 762-63 (1969) (requiring no particularized suspicion for searches under the search incident to arrest exception).

The "border search exception" is one such "longstanding, historically recognized exception" that permits warrantless searches at the border and international ports of entry. *United States v. Ramsey*, 431 U.S. 606, 621 (1977) (internal quotations omitted). Most searches at the border are "routine" ones that require no particularized suspicion; only highly invasive searches *might* give rise to a requirement of "reasonable suspicion." *Montoya de Hernandez*, 473 U.S. at 538, 541 n.4. Thus, the question that has divided the circuit courts is what degree of particularized suspicion, if any, must agents have to conduct a forensic digital search under the border exception?

The Ninth Circuit has announced the most stringent standard: border agents may conduct a forensic digital search only when they have reasonable suspicion that the search will uncover digital contraband *itself* – not even evidence of smuggling contraband or other crimes. *United States v. Cano*, 934 F.3d 1002, 1018 (9th Cir. 2019). First, in *United States v. Cotterman*, over a vigorous dissent, an en banc court held that forensic border searches require reasonable suspicion. 709 F.3d 952, 957 (9th Cir. 2013). However, because border agents in that case had reasonable cause to suspect that the defendant had child pornography on his devices, the en banc panel did not decide whether other grounds for suspicion would support a search. *Id.* The Ninth Circuit picked that question back up in *Cano* and answered it in the negative: a forensic search is only permissible on suspicion that it will turn up actual digital contraband. 934 F.3d at 1018.

The Fourth Circuit adopted a wider view of the acceptable bases for suspicion and held that forensic searches are valid when conducted on reasonable suspicion of border-related or "transnational" criminal activity. *United States v. Aigbekaen*, 943 F.3d 713, 721 (4th Cir. 2019). Previously, in *United States v. Kolsuz*, it held that border agents must have reasonable suspicion of some offense with a "nexus" to the justifications underlying the border search exception to the

warrant requirement. 890 F.3d 133, 143 (4th Cir. 2018); *but see Aigbekaen*, 943 F.3d at 728-29 (Richardson, J., concurring) (arguing that *Kolsuz* merely noted the *possibility* of a nexus requirement but did not affirmatively adopt one). However, *Kolsuz* offered little regarding the contours of that "nexus" requirement; the facts gave agents reason to suspect that the defendant was attempting to export illegal firearms, which the court concluded was sufficient justification "on any account of a 'nexus' requirement." 890 F.3d at 143. The Fourth Circuit provided further explication in *Aigbekaen*, where it announced, again over vigorous disagreement, a distinction between mere "domestic" crimes, which lacked a "nexus" and "transnational" ones, which satisfied the requirement. 943 F.3d at 721. Thus, agents could search for evidence, not just contraband, and they could also search on suspicion of crimes beyond just smuggling – but still only those crimes that are "transnational." *Id.*; *Kolsuz*, 890 F.3d at 143 (permitting a search to look for evidence).

In the instant case, a unanimous panel of the Tenth Circuit held that reasonable suspicion of *any* criminal activity would justify a forensic search at the border. R. at 13. It declined to definitively hold that reasonable suspicion was necessary. R. at 11. However, it rejected petitioner's argument to adopt a *Cano*-like standard, instead agreeing with the district court that reasonable suspicion of all types of criminal activity suffices to justify forensic searches. R. at 13. It reasoned that there was no justification to hold otherwise, as "[t]he Fourth Amendment does not require [law enforcement] officers to close their eyes to suspicious circumstances." R. at 13 (internal quotations and citation omitted). Accordingly, the panel affirmed the denial of petitioner's motion to suppress, determining that agents possessed reasonable suspicion that he may have been engaged in criminal activity. R. at 11, 13.

Finally, the Eleventh Circuit in *United States v. Touset* held that border agents may conduct a forensic digital search without any particularized suspicion. 890 F.3d 1227, 1233 (11th Cir. 2018). The Eleventh Circuit noted that neither it, nor this Court, had ever required reasonable suspicion for a search of property at the border. *Id. Touset* reasoned that the factors that could make a search so invasive as to demand reasonable suspicion were relevant to searches of persons – not property – and given the paramount government interest in protecting the integrity of the border, it declined to afford "special protection" to those who happen to store illicit property like child pornography in digital form. *Id.* at 1234-36.

Thus, this case presents the opportunity to resolve the discord among the circuits and definitively clarify what standard of suspicion is necessary for officials to conduct a forensic digital search at the border.

SUMMARY OF ARGUMENT

"[T]he Fourth Amendment balance between the interests of the Government and the privacy right of the individual [is] struck much more favorable to the Government at the border." *Montoya de Hernandez*, 473 U.S. at 540. This Court has never required particularized suspicion for a border search of property, and this case should be no different. Accordingly, this Court should adopt the *Touset* standard and hold that forensic digital searches at the border are reasonable with no particularized suspicion. However, if this Court determines that forensic border searches must be supported by particularized suspicion, it should affirm the conclusion of the panel below that reasonable suspicion of *any* criminal activity justifies the search.

At the border, individuals have a diminished expectation of privacy, while the government interest in monitoring the people and property entering the country is "at its zenith." *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004); *see also Montoya de Hernandez*, 473 U.S. at 539. Thus, most border searches are reasonable without suspicion. This Court has

suggested that some border searches *might* be so invasive as to require particularized suspicion. *Flores-Montano*, 541 U.S. at 152, 155-56; *Montoya de Hernandez*, 473 U.S. at 541 n.4. But a forensic digital search is not such a search. It is true that in *Riley v. California* this Court recognized the heightened privacy interest individuals have in their digital devices given their pervasive role in modern life. 573 U.S. 373, 385-86 (2014). But what separates this case is that unlike *Riley*'s search incident to arrest context, where searches of digital data do not further the government interests at play, in the border context, digital searches are vital to carrying out the government purposes underlying the border exception. *Id.* at 386-88. Thus, this heightened privacy interest is counterbalanced – and ultimately outweighed – by heightened government interests, and like the vast majority of border searches, forensic digital searches are reasonable without particularized suspicion.

Alternatively, if forensic digital searches require some degree of particularized suspicion, the border exception's precedent, purposes, and practical realities all illustrate that reasonable suspicion of any criminal activity is sufficient to justify a search. The Ninth and Fourth Circuits employ arbitrary limitations on the permissible bases for suspicion; the former requires suspicion of finding contraband *itself*, while the latter requires suspicion of a "transnational" crime. *Cano*, 934 F.3d at 1018; *Aigbekaen*, 943 F.3d at 721. Analogous Fourth Amendment contexts contain no artificial limits that force officials to willfully blind themselves to certain crimes. These standards also misapprehend the rationales for the border search exception and fail to appreciate how searches for all forms of crime serve its purposes. Further, *Cano* and *Aigbekaen* offer little clarity. If adopted, agents would have to make impossible determinations as to which searches are permissible, inhibiting them from discharging their important duties to protect our border.

This Court has made clear that such murky doctrinal tests have no place at the border. *Flores-Montano*, 541 U.S. at 152.

ARGUMENT

I. Searches of digital devices at the border do not require particularized suspicion.

This Court has often reiterated that at the border, the balance of interests underlying the Fourth Amendment's reasonableness requirement is tilted heavily towards the government. *Montoya de Hernandez*, 473 U.S. at 540. Individuals have a diminished privacy interest, and the government has a heightened security interest. *Id.* at 539-40. Accordingly, "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. Though forensic digital searches involve a greater intrusion on individual privacy, that still does not overcome the paramount government interest served by such searches. The government can often conduct searches at the border that would be impermissible in the interior. *Carroll v. United States*, 267 U.S. at 154. Thus, the border search doctrine makes clear that forensic searches are reasonable even without particularized suspicion.

A. Non-invasive border searches do not require any particularized suspicion.

"The touchstone of the Fourth Amendment is reasonableness." *Florida v. Jimeno*, 500 U.S. 248, 250 (1991). This Court's precedent illustrates that searches of property at the border are reasonable even without suspicion; only the most invasive searches might demand reasonable suspicion of criminal activity.

The Fourth Amendment commands only that searches and seizures not be "unreasonable." U.S. Const. Amend IV; *see Jimeno*, 500 U.S. at 250. Thus, searches and seizures conducted without a warrant are valid so long as they are reasonable. Reasonableness is

a fact-specific inquiry evaluated by balancing individual privacy interests against the government's interests based on the totality of the circumstances. *Montoya de Hernandez,* 473 U.S. at 537; *see also Ohio v. Robinette*, 519 U.S. 33, 39 (1996). As a result, the level of suspicion that is required for government officials to conduct a warrantless search varies by context. In some, officials must have probable cause; in other contexts, officials need only a lesser degree of suspicion, and still in others, they may search freely with no particularized suspicion whatsoever. *See, e.g., Carroll*, 267 U.S. at 154 (requiring probable cause to search automobiles during traffic stops); *New Jersey v. T.L.O.*, 469 U.S. 325, 341-42 (1985) (requiring reasonable suspicion to search students in schools); *Chimel v. California*, 395 U.S. 752, 762-63 (requiring no particularized suspicion to search the person of arrestees during their arrest).

At the border, the balancing of interests underlying the reasonableness inquiry is "struck much more favorably to the government." *Montoya de Hernandez*, 473 U.S. at 540. For one, this Court has recognized that an individual has a significantly diminished expectation of privacy at the border, where searches of person and property are commonplace. *Id.* at 539. Further, border searches are founded not on traditional law enforcement justifications, but rather the federal government's sovereign power to determine who and what enter the country. *Id.* at 537; *Carroll*, 267 U.S. at 154. Congress has delegated its plenary customs and immigration authority to give the Executive broad powers to screen entrants, including through searches of their effects. *See Montoya de Hernandez*, 473 U.S. at 537*; Ramsey,* 431 U.S. at 616; *Boyd v. United States*, 116 U.S. 616, 623 (1886).

Because this balance of interests is so tilted towards the government, border agents may need particularized suspicion only in rare cases when they conduct highly intrusive searches or seizures. *United States v. Montoya de Hernandez* illustrates this point. 473 U.S. 541. There,

customs officials suspected a traveler from Bogota of smuggling drugs in her alimentary canal and detained her for nearly sixteen hours to monitor any bowel movements before seeking a warrant for an x-ray and rectal examination. *Id.* at 534-35. After a magistrate issued the warrant, the rectal examination produced a balloon of cocaine, and the traveler was formally arrested. *Id.* at 535-36. This Court held that her lengthy detention – an unusually intrusive *seizure* – required reasonable suspicion of smuggling, which customs agents justifiably had under the circumstances. *Id.* at 541-42. However, as to *searches*, this Court reiterated that at the border, "[r]outine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant," while explicitly reserving the question of what level of suspicion, if any, was required for unusually intrusive, nonroutine searches. *Id.* at 538, 541 n. 4.

B. Forensic searches of digital devices are non-invasive searches.

This Court has never deemed any border search of property invasive enough to require particularized suspicion. And while digital devices play an increasingly large role in our lives, their search is not so intrusive on individual privacy interests as to overcome the government's interest in preserving the integrity of the border. Thus, suspicionless forensic digital searches fit comfortably within existing border search doctrine.

1. Forensic digital searches are not invasive enough in any of the three respects that could give rise to a requirement of particularized suspicion.

In *United States v. Flores-Montano*, this Court identified three potential ways in which searches may be invasive enough to require particularized suspicion: if they severely intrude on dignity or privacy or are highly destructive.[1] 541 U.S. 149, 152, 155-56. *Flores-Montano*

[1] In a footnote, this Court also used the phrase "particularly offensive manner" to describe certain searches that could potentially be deemed unreasonable. *Flores-Montano*, 541 U.S. 154 n.2 (quoting *Ramsey*, 431 U.S. at 618 n.13) (internal quotation omitted). Some have interpreted this as articulating yet another category of invasive search.

affirmed the validity of the suspicionless disassembly and inspection of a motorist's gas tank at a border crossing. *Id.* at 155. This Court acknowledged that highly intrusive searches of one's person "might" require greater suspicion but noted that vehicular searches did not implicate the dignity or privacy interests that would give rise to such a requirement. *Id.* at 152. And further, even if some searches of property *could* be so destructive as to demand particularized suspicion, the gas tank at issue was fully reassembled and thus unharmed. *Id.* at 155-56.

Forensic searches of digital devices are do not implicate dignity interests, are not destructive, and though they implicate privacy interests, they do not rise to the level invasiveness that would overcome the government interests at stake. Thus, border agents may conduct such searches freely without any particularized suspicion.

(a) Digital searches do not involve bodily intrusions and therefore do not implicate dignity interests.

Searches of digital devices involve no incursion on bodily integrity, and thus they do not intrude on a traveler's dignity. The dignity interest embodied by the Fourth Amendment centers on the extent to which a search or seizure violates an individual's bodily autonomy. For example, in *Schmerber v. California*, the Fourth Amendment analysis of a warrantless, compulsory blood test of a suspected drunk driver focused on the impact to human dignity of "intrusions beyond the body's surface." 384 U.S. 757, 769-70 (1966). Similarly, in *Skinner v. Railway Labor Executives' Ass'n*, this Court sharply divided on how far suspicionless blood and urine tests of railway employees invaded their bodily dignity. 489 U.S. 602, 616-17 (1989); *id.* at 644-46 (Marshall, J., dissenting). And Justice Brennan's dissent in *Montoya de Hernandez* was premised

See, e.g. Aigbekaen, 943 F.3d at 728 (Richardson, J., concurring). However, the footnote primarily discusses searches using exploratory drilling and their destructiveness. *Flores-Montano*, 541 U.S. 154 n.2. Thus, for the analysis that follows, it is assumed that "particularly offensive manner" searches are not a separate category of invasive searches but are merely destructive searches by another name.

in part on his view of the dignity impact of being detained subject to a monitored bowel movement. 473 U.S. at 560-62 (Brennan, J., dissenting). Searches of laptops and cell phones do not implicate these considerations or the dignity interest protected by the Fourth Amendment.

(b) Forensic digital searches do not harm the device and thus do not implicate the owner's interest in the property being preserved.

Forensic digital searches are not destructive. Though they temporarily dispossess the owner of their property, so do all searches. Even where they are lengthy, like in this case, that is mainly the result of the traveler's refusal to consent to a faster process, and decisions of the device owner do not suddenly make a search unreasonable. A search that merely temporarily denies the owner's possession – with no permanent damage – is not so destructive as to potentially require particularized suspicion.

Forensic searches do not harm the device. Like the one in this case, forensic searches often begin with agents making a digital copy of the device to avoid altering any data on the original or causing any digital damage. R. at 22. And the basic handling and operation of the device in connection with the search is unlikely to cause any physical damage. The search ultimately leaves the device no worse for wear.

While forensic searches do temporarily impair the owner's possessory interest, that does not amount to the sort of property destruction that could demand a higher level of suspicion to justify the search. *See Flores-Montano*, 541 U.S. at 155-56. For one, *all* property searches temporarily deny the owner's possession, so that alone cannot justify treating forensic digital searches more stringently than all other border searches of property. Although agents disassembling, inspecting, and reassembling the gas tank in *Flores-Montano* briefly interrupted the driver's possession of the vehicle, that minor interference did not overcome the government's

interest in protecting the border. *Id.* at 155. By the same token, a device owner's temporary loss of possession does not overcome the weighty government interest.

The fact that a forensic digital search may take longer than a gas tank search makes no difference. Forensic searches may take days or weeks when the owner refuses to provide the device's password and forces agents to "crack" it themselves, as the petitioner did here. R. at 20-21, 24. Providing a password would greatly reduce the length of time required by the search. *Montoya de Hernandez* shows that when an individual refuses to consent to a faster procedure to conclude the search or seizure, the government's inspection does not become unreasonable simply because it was forced to use the lengthier method. 473 U.S. at 543 (discussing the respondent's refusal to agree to a faster x-ray search). The mere temporary dispossession of one's device without any damage to the device or its contents is not enough to require a greater level of suspicion for the search.

(c) While forensic digital searches involve greater intrusions on privacy, given the minimal expectation of privacy and weighty government interests at the border, they are not invasive enough to require particularized suspicion.

Forensic digital searches impose a more significant intrusion on one's personal privacy, but they are not so invasive as to overcome the government's paramount interest or require more suspicion than all other border searches of property. Undoubtedly, laptops and smartphones play important roles in our lives, but that does not mean that their search is uniquely invasive in a setting where travelers have a greatly diminished expectation of privacy and the government has a substantial interest in protecting the integrity of the border. *Id.* at 539.

In a case regarding the "search incident to arrest" exception to the warrant requirement, this Court recognized the "pervasive and insistent" nature of cell phones in modern life and the large quantities of information they carry. *Riley*, 573 U.S. at 385-86. Though *Riley* dealt only with cell phones, the same is assuredly true of other digital devices like laptops. For most

searches incident to arrest, officers may search with no warrant and no particularized suspicion. *Chimel v. California*, 395 U.S. at 762-63. But when it comes to cell phones, *Riley* established that police may not conduct a warrantless search of their digital contents incident to the arrest. *Riley*, 573 U.S. at 386. However, neither the terms of *Riley's* holding nor the logic of its reasoning suggest that digital searches at the border require particularized suspicion.

First, *Riley* was careful to cabin its holding to searches incident to arrest. "[E]ven though the search incident arrest exception does not apply to cell phones, other case-specific exceptions may still justify a warrantless search of a particular phone." *Id.* at 401-02. Thus, though more stringent requirements apply to digital searches incident to arrest, it does not follow that the same is true for border searches.

Further, *Riley* rests on the notion that searches of cellular data involve heightened individual privacy interests and diminished government interests compared to other searches incident to arrest. But that is not true of digital border searches relative to other border searches.

Riley articulated a heightened individual privacy interest by citing the different "quantitative" and "qualitative" nature of cellular data compared to objects normally found in an arrest search. *Id.* at 393. This Court noted that people "cannot lug around" large quantities of personal information on their person, and if they did, they would have to "drag behind them a trunk." *Id.* at 393-94. But travelers at the border usually come with trunks and suitcases full of personal effects and files or documents. Digital devices may still hold more, but the disparity is far less than that of the search incident to arrest context, where arrestees typically have trivial amounts of information on their person.

Similarly, the difference in the qualitative nature of the information that digital searches reveal is much greater in the arrest context than at the border. *Riley* noted that cellular data may

reveal private or sensitive material, such as "[h]istorical location information" or health information through "a search for certain symptoms of disease." *Id.* at 395-96. Basic searches through an arrestee's pockets as part of their arrest would likely not reveal such material.

By contrast, typical border searches of a traveler's luggage and effects often implicate private or sensitive material. The very examples from *Riley* are illustrative. A basic suitcase search could reveal a traveler's medications and thus disclose some health information. And getting historical location information is one of the primary purposes of border checkpoints – as this case well illustrates, travelers must reveal the extent of their foreign travels to help officials determine if they pose any security risk. *See* R. at 18-20 (discussing Agent Allen's questioning of petitioner about his travels). These routine border searches are reasonable in spite of the sensitive information they may uncover because the expectation of privacy is simply less at the border. *Montoya de Hernandez*, 473 U.S. at 450. That is just as true for digital contents.

On the other side of the balancing equation, digital searches incident to arrest do not serve the government interests underlying that exception, but they do still further government interests at the border. *Riley* noted that the search incident to arrest exception is founded on two government interests: preventing harm to officers effecting the arrest and preventing destruction of evidence. 573 U.S. at 386. Since digital data cannot be used as a weapon against arresting officers, and since officers can secure an arrestee's cell phone to prevent destruction of any digital evidence, searches of cellular data do not serve the government interests justifying the exception. *Id.* at 387-88.

By contrast, digital searches at the border still serve the government interest underlying the warrant exception: regulating "who and what may enter the country." *Ramsey*, 431 U.S. at

620. Officials at the border are charged with blocking efforts to import contraband, denying entry to ineligible persons, and protecting national security. *See Aigbekaen*, 943 F.3d at 721.

Forensic digital searches further all of these missions. As this case illustrates, contraband itself can be digital, such as the child pornography that the petitioner tried to smuggle on his laptop. R. at 23. Indeed, forensic searches are likely the *only* way that agents may detect and interdict such digital contraband. Forensic searches can also help shed light on whether a traveler is eligible for entry into the country. Travelers may lie or be evasive about their foreign travels, like the petitioner here. R. at 20-21. Or they may try to use a false identity to slip through immigration controls. In a single day, U.S. Customs and Border Protection typically intercepts 18 fraudulent identity documents and encounters hundreds of inadmissible persons at ports of entry. CBP, *Snapshot*. Forensic digital searches help these efforts to ferret out deception and ensure that only authorized persons are admitted for entry. The government's national security interest is even more compelling: border officials are the primary line of defense against travelers to the United States who would seek to commit acts of violence or terror. This Court has recognized that the "Government's interest in preventing the entry of unwanted persons and effects is at is zenith at the international border." *Flores-Montano*, 541 U.S. at 152. Forensic digital searches ensure that border agents can carry out that important duty.

Riley excluded cellular data from the search incident to arrest doctrine because digital searches are unique compared to all other arrest searches. They are far more intrusive on individual privacy interests and far less helpful to the government interests justifying such searches. But digital searches do not impose a dramatically greater invasion of privacy because travelers have a minimal expectation of privacy at the border. *See id.* at 154. And they are vital to the government interest that justifies the border search doctrine: policing "who and what may

enter the country". *Ramsey*, 431 U.S. at 620. Thus, forensic digital searches are like other routine border searches, which require no suspicion because the balance of interests is so heavily tilted towards the government at the border. *Montoya de Hernandez*, 473 U.S. at 538, 540. Accordingly, forensic digital searches should require no particularized suspicion.

2. Suspicionless forensic digital searches fit comfortably within the existing legal framework – requiring particularized suspicion would lead to anomalous results both doctrinally and practically.

In requiring reasonable suspicion for forensic digital searches, the Ninth Circuit argued that doing so was necessary to avoid inconsistencies in Fourth Amendment jurisprudence. But in fact, the opposite is true. Suspicionless searches of property at the border are well established, even though those same searches might be impermissible elsewhere. Requiring particularized suspicion for forensic digital searches would be anomalous.

In *Cano*, the Ninth Circuit thought that border agents must have reasonable suspicion that the device contains digital contraband to justify a forensic search because ruling otherwise would erode this Court's decision in *Riley*. 934 F.3d at 1020. "Were we to give the government unfettered access to cell phones, we would enable to the government to evade the protections laid out in *Riley* on the mere basis that the searches occurred at the border." *Id.* (internal citations and quotation omitted).

However, this argument misapprehends the relationship of different exceptions to the warrant requirement. Permitting forensic border searches without suspicion would do nothing to undermine *Riley*. *Riley* does not stand for a generalized protection of digital data; it expressly cabined its holding to the search incident to arrest exception and cautioned against reading it as making cell phones "immune from search." 573 U.S. at 401-02.

Rather, permitting suspicionless forensic border searches comports with a centerpiece of our Fourth Amendment law: that different levels of suspicion are required for different contexts.

The border is simply one of several contexts where the diminished expectation of privacy and weighty government interests permit searches on lesser suspicion than would otherwise be required. *Montoya de Hernandez*, 473 U.S. at 538-39; *see also Florence v. Bd. of Chosen Freeholders*, 566 U.S. 318, 339 (2012) (requiring lesser suspicion in jails and prisons); *T.L.O.*, 469 U.S. at 340-41 (requiring lesser suspicion in schools) ("The school setting also requires some modification of the level of suspicion of illicit activity needed to justify a search.").

The foundational *Carroll* case proves this point. There, this Court articulated the automobile exception to the warrant requirement and required probable cause to search vehicles during traffic stops. 267 U.S. at 154. Yet in the very sentence that preceded that holding, *Carroll* explained that at the border, the same vehicle may be searched without any suspicion. *Id.; see also Flores-Montano*, 541 U.S. at 155 (reaffirming the validity of suspicionless vehicular searches). Clearly, the *Carroll* court did not think it was illogical or anomalous to permit border searches on less suspicion than would be required to conduct the same search in the interior. That principle applies with equal force to forensic digital searches.

Quite contrary to *Cano's* reasoning, requiring particularized suspicion to conduct a forensic border search would be unusual, both from a doctrinal and practical perspective. For one, this Court has never required any particularized suspicion for a border search of property. *Montoya de Hernandez* spoke only to a particularly invasive *seizure* – not a search – and the language in *Flores-Montano* that suggested that some searches *might* be invasive enough to demand greater suspicion was largely focused on intrusive searches of one's *person*. 473 U.S. at 541 n. 4; 541 U.S. at 152 ("reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the *person* [] simply do not carry over to vehicles") (emphasis added).

Further, a reasonable suspicion requirement would make little sense given the Ninth Circuit's related precedent. *Cano* that "manual" searches of cellular data, a so-called "quick and unintrusive look," may be done without suspicion. 934 F.3d at 1015; *see also Cotterman*, 709 F.3d at 967 (holding the same for laptops). Thus, it seemed to draw a dividing line between relatively brief searches in which an agent physically operates the device to search its data and more extensive searches, potentially with digital tools like the ones used here assisting in the search. R. at 22-23. Of course, an agent "manually" searching a device could still come across highly personal, sensitive information. Thus, the only logical explanation for this distinction is that forensic searches are more invasive because they have a greater *likelihood* of revealing such sensitive material.

While the marginal likelihood of forensic searches uncovering personal material may amount to a greater intrusion on individual privacy, it still does not support treating forensic searches differently given the government interest in a thorough search. Consider the interdiction of digital contraband, like the child pornography the petitioner tried to import here. R. at 23-24. Brief "manual" searches will rarely, if ever, uncover such contraband given the lengths smugglers would go to in order to hide it. Thus, a forensic search is often the only way to interdict this contraband. *Flores-Montano* is analogous. The cursory initial inspection where agents knocked on the gas tank cannot definitively confirm that contraband is hidden inside; the more extensive disassembly and search is needed. *See* 451 U.S. at 151. Just as no particularized suspicion was required for the former search, neither was it required for the latter, even though it was more invasive. *Id.* at 155. Similarly, even if forensic searches involve a greater privacy invasion, there is *also* a greater government interest in conducting the thorough search necessary

to accomplish its purposes. Thus, the Fourth Amendment balancing still ultimately lies in the government's favor.

Moreover, requiring reasonable suspicion for forensic digital searches would yield odd practical results. It would privilege material simply because it is digital, when that same material could be examined in a suspicionless search if it were in physical form. Agents could search a vehicle attempting to drive into the country without any suspicion, even if were filled with sensitive personal effects. *See Touset,* 890 F.3d at 1233. So too could they conduct a suspicionless search of the suitcase of a traveler arriving from abroad, even if it happens to be full of personal documents. *See id.* It thus makes little sense to afford the same information extra protection because it happens to be in electronic form. If border officers are to keep out contraband like child pornography, it makes little sense to require more for digital searches at the very time when that contraband is increasingly being trafficked in digital form. *Id.* at 1235-36.

II. Even if border agents must have reasonable suspicion for a forensic digital search, that suspicion need not bear any connection to a particular *type* of criminal activity.

If this Court decides that forensic digital searches must be supported by particularized suspicion, it should affirm the standard adopted here by the Tenth Circuit that requires agents to have reasonable suspicion of any criminal activity. R. at 13. The standards articulated by the Ninth and Fourth Circuits that require agents to have suspicion of specific types of crimes run against Fourth Amendment precedent, misunderstand the justifications underlying the border exception, and ignore the practical realities of protecting the nation's border.

A. There is no precedential support for any "nexus" requirement.

If forensic digital searches must have some particularized suspicion, it is clear that only reasonable suspicion is required, not probable cause. But reasonable suspicion as to what? Contrary to the decision below, the Ninth and Fourth Circuits require that the suspicion bear a

connection to certain types of crimes. A survey of Fourth Amendment contexts that require reasonable suspicion illustrates that such a requirement is untethered from precedent.

If any particularized suspicion is required, border agents need only reasonable suspicion. This Court made clear that in *Montoya de Hernandez* that in the Fourth Amendment context, there are two standards of particularized suspicion: reasonable suspicion and probable cause. 473 U.S. at 540-41. This Court has never required probable cause for a search made under the border exception, and in *Ramsey*, it reiterated and reaffirmed the "longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless 'reasonable.'" 431 U.S. at 619. For all the ink spilled by the circuit courts on this issue, not one of them has held that probable cause is required – even the most stringent of them, the Ninth Circuit, requires only reasonable suspicion. *Cotterman*, 709 F.3d at 968; *Cano*, 934 F.3d at 1016.

The panel below held that border agents need reasonable suspicion of any criminal activity, while the Fourth and Ninth Circuits limit the types of crimes that will support a search. R. at 13; *Aigbekaen*, 943 F.3d at 721; *Cano*, 934 F.3d at 1017. The Fourth Circuit requires border agents to have reasonable suspicion of an offense with some "nexus to the border exception's purposes." *Aigbekaen*, 943 F.3d at 721. The Ninth Circuit, though it did not use the term "nexus," essentially applied a heightened nexus requirement: searches are only justified on reasonable suspicion of turning up digital contraband itself, not even evidence of other border-related crimes. *Cano*, 934 F.3d at 1017.

Precedent provides no support for this *ad hoc* limitation. Other Fourth Amendment contexts illustrate that warrantless search authority is not arbitrarily circumscribed. Undoubtedly, the purposes underlying a warrant exception inform the permissible scope of a search conducted pursuant to that exception. *Riley*, 573 U.S. at 386. But it is illogical and unprecedented to apply

that principle woodenly and force government agents to "close their eyes to suspicious circumstances." R. at 13 (quoting *United States v. Johnson*, 895 F.2d 693, 696 (10th Cir. 1990)). This Court has not done so in other contexts. In schools, for example, officials may conduct a search when they have reasonable suspicion that a student has violated *any* law or school rule, not merely some limited subset of education-related laws. *T.L.O.*, 469 U.S. at 341-42. And officials may search when they suspect that they will find *evidence* of a violation, not merely contraband prohibited within school walls. *Id.* Similarly, the automobile exception allows officers to search vehicles if they have probable cause to suspect criminal activity, including evidence thereof. *Carroll*, 267 U.S. at 154, 158-59. The search authority does not merely apply to a narrow class of vehicular or road-related offenses. Thus, the Ninth Circuit's requirement that forensic digital searches be for contraband alone, not evidence, is without support. *Cano*, 934 F.3d at 1017. The same is true of the Fourth Circuit's standard arbitrarily limiting the potential crimes that may provide grounds for reasonable suspicion. *Aigbekaen*, 943 F.3d at 721.

B. The justifications underlying the border search exception do not imply that only certain types of criminal activity are relevant.

The Fourth and the Ninth Circuits argue that their narrow standards are the product of the border exception's purposes. But this analysis is flawed. The Ninth Circuit errs by using a cramped notion of the border exception's purposes. And while the Fourth Circuit has a more accurate view of the justifications for the exception, it fails to appreciate the ways that searches based on reasonable suspicion of *any* criminal activity would serve those purposes.

1. Even on *Cano*'s own mistaken view of the purposes of the border exception, it is arbitrary to limit forensic searches to only those for contraband itself.

The Ninth Circuit limited searches to those for digital contraband because it deemed the detection of contraband to be "'the strongest historic rationale for the border-search exception.'" *Cano*, 934 F.3d at 1018 (quoting *United States v. Molina-Isidoro*, 884 F.3d 287, 295 (5th Cir.

2018) (Costa, J., specially concurring). But this argument is mistaken in both its premises and conclusion.

It is unwarranted to conclude that detecting contraband is the "strongest" justification for the border search exception. Certainly, it is an important one – for example, each day at the border, agents seize nearly 4,000 pounds of narcotics. CBP, *Snapshot*. But border agents are charged with many other duties. Fundamentally, they must police "who and what may enter." *Ramsey*, 431 U.S. at 620. This includes not just a customs and interdiction component, but also an immigration component and a national security component, as even the Fourth Circuit recognized. *Aigbekaen*, 943 F.3d at 720; CBP, *Snapshot* (articulating a mission of "protecting the public from dangerous people and materials"). The Ninth Circuit singles out one of the many overlapping responsibilities of those officials protecting our border, and in doing so, makes an inappropriate and unsupported policy judgment.

Moreover, even accepting the Ninth Circuit's notion that intercepting contraband is the "strongest" purpose underlying the border search exception, that still does not imply that it is the *only* purpose that can support a forensic digital search. *Cano* made much of the fact that this Court's border search cases all involve the detection of contraband. 934 F.3d at 1018. Yet, this fact is unsurprising – it merely reflects how frequently agents intercept narcotics and other illicit material. It makes little sense to take that fact and therefore deduce that forensic searches can only be for contraband. Quite ironically, *Cano*'s conclusion amounts to punishing border agents for their success in interdicting contraband. The search incident to arrest exception is illustrative. Two rationales support it: protecting officers from potential weapons and preventing destruction of potential evidence. *Riley*, 573 U.S. at 386. One may regard the former purpose of protecting officers as "stronger," yet if that meant that officers may exclusively search for weapons, it

would effectively erase the latter purpose. *Cano* would similarly erase all but one of the justifications underlying the border exception.

Finally, even if intercepting contraband were the sole purpose of the border exception, it still would not follow that forensic searches must be limited to looking for contraband itself. Consider agents who, in the routine search of a traveler's luggage, come across a suspicious package that they believe contains narcotics. A forensic search of the traveler's cell phone could provide the evidence needed to confirm their suspicion. Yet *Cano* closes off this investigative avenue. Or suppose that agents are alerted that a traveler visits online communities known for distribution of child pornography. They would be able to forensically search the traveler's laptop to determine whether it contains child pornography. But under *Cano*, they could not search the traveler's communications with other members of that online community, even though those communications could alert the agents to the presence or even the very location of child pornography on the device. The Ninth Circuit forces border agents to be willfully blind; *Cano* imposes a restraint on border search authority that is rendered artificial by the very purpose offered to justify it.

2. *Aigbekaen* ignores the fact that searches for all types of criminal activity serve the justifications for the border exception that it identifies.

The Fourth Circuit was correct to acknowledge a broader array of justifications for the border search exception, but it failed to fully appreciate how forensic digital searches relate to those justifications. A search that is supported by reasonable suspicion of *any* crime, not merely border-related offenses, furthers the border exception's purposes.

In essence, *Aigbekaen* held that agents must have reasonable suspicion of some "transnational" crime. 943 F.3d at 721. The Fourth Circuit based its standard on this Court's language from *Riley* that cautioned that searches under an exception to the warrant requirement

must not be "untether[ed]" from the exception's justifications. *Id.* at 720 (quoting *Riley*, 573 U.S. at 386). It characterized the purposes underlying the border search exception as "protecting national security, collecting duties, blocking the entry of unwanted persons, [and] disrupting efforts to export or import contraband." *Id.* at 721. Thus, in the Fourth Circuit's view, agents had to possess reasonable suspicion of an offense with a "nexus" to one of those purposes. *Id.* As a general matter, this statement of the justifications for the border exception is accurate. However, the effect of *Aigbekaen*'s "nexus" requirement is to limit the universe of crimes that may support reasonable suspicion to ones that are "transnational" – not mere "domestic" crimes, as it characterized the offense in that case. *Id.*

Aigbekaen ignores the fact that searches based on any criminal activity, not just the transnational variety, further the purposes of the border exception. For one, as previously discussed, the purposes of policing "who and what may enter the country" demands broad latitude to conduct forensic searches. *Ramsey*, 431 U.S. at 620; *see supra* Section I.B.1.c.

Consider one purpose of the border exception that the Fourth Circuit identifies: preventing "unwanted persons" from being admitted. *Aigbekaen*, 943 F.3d at 721; *see also Flores-Montano*, 541 U.S. at 152 (referring to the government interest in "preventing the entry of unwanted persons"). If border agents reasonably suspect that a traveler may have committed some "domestic" crime in their country of origin, surely that suspicion is relevant to whether they are eligible to be and should be admitted to the country. Yet *Aigbekaen* forbids agents from using a forensic digital search to investigate further, frustrating both the agents' ability to do their job and the border exception's purpose. The same logic applies even when the incoming traveler is an American suspected of "domestic" crimes committed in the United States. This is a common occurrence: agents apprehend thousands of criminally wanted persons at ports of entry

every year. CBP, *Snapshot*. But wanted individuals are likely to try and conceal their identity. If border agents suspect a traveler is a criminally wanted individual using a false identity, they need forensic digital searches to determine whether that traveler is indeed wanted or should admitted to roam freely about the interior.

Similarly, searches on suspicion of "domestic" crimes also serve the border exception's purpose of protecting national security. Consider an individual who agents reasonably suspect was involved with a bombing in a foreign country and is traveling to the U.S., intending to do the same. The mere fact that an individual intends to commit the same crime in multiple countries does not inherently make those crimes "transnational." Thus, unless the foreign bombing had some eminently "transnational" component, agents would be powerless to conduct the forensic digital search that could uncover the traveler's plot and prevent such a bombing on U.S. soil. Ultimately, much like the Ninth Circuit's erroneous standard, *Aigbekaen* artificially limits the crimes that may provide the grounds for suspicion and, in doing so, frustrates the border exception's purposes.

C. *Cano* and *Aigbekaen* both create standards that are unworkable in practice.

The arbitrary limitations that the Ninth and Fourth Circuits impose will lead to uncertainty about which searches are permissible at the border. Agents will not know when they may conduct forensic digital searches, with the threat of an action for personal damages looming against them. Reviewing courts will also struggle with questions of which searches are permissible under these standards, requiring this Court to again step in and resolve circuit splits and confusion.

It is well-established that agents who violate the Fourth Amendment by conducting an unreasonable search or seizure are subject to personal liability in a *Bivens* action, named for case establishing that principle. *Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics*,

403 U.S. 388, 389 (1971). It is true that the qualified immunity doctrine protects officials from liability when the contours of constitutional rights are not "clearly established." *Harlow v. Fitzgerald*, 457 U.S. 800, 818 (1982). But as this four-way circuit split case illustrates, courts may differ greatly about what the "clearly established" principles of Fourth Amendment law are. Ultimately, uncertainty creates risk of liability for agents. And importantly, even if that risk turns out to be unfounded because the protections of qualified immunity apply, it may nonetheless chill border agents from making the difficult decisions necessary to discharge their duties. *Cotterman*, 709 F.3d at 979-80 (Callahan, J., dissenting). It is far better to avoid such uncertainties in the first place. *Aigbekaen*, 943 F.3d at 732-33 (Richardson, J., dissenting).

The *Cano* standard will require border agents to make impossible determinations of when a traveler's devices might contain digital contraband. For example, agents may reasonably suspect that a traveler possesses child pornography, but they may not know whether it is in physical or digital form. An agent must make the decision of whether to limit their search to physical inspection, thus turning a blind eye to the digital form that child pornography is increasingly likely to take, or conduct a forensic search, thus risking *Bivens* liability. Even in instances where agents have reasonable suspicion that a traveler has digital contraband, does that apply to all of the traveler's devices – laptops, cell phones, and tablets alike? The Ninth Circuit dismissed concerns over its lack of doctrinal clarity, proclaiming its "confidence" in border agents to determine the scope of their authority. *Cotterman*, 709 F.3d at 967. That confidence will be cold comfort to agents operating with little guidance under threat of a *Bivens* action.

Similarly, *Aigbekaen* forces border agents to determine whether a potential crime is "transnational" at a moment when they are short on facts. *Aigbekaen* itself illustrates the slippery nature of the standard it articulates. There, the defendant was suspected of sex trafficking minors.

Aigbekaen, 943 F.3d at 717. The defendant was returning from abroad, and sex trafficking is commonly conducted across international lines. *Id.* at 733 (Richardson, J., dissenting). Yet, the Fourth Circuit concluded that the search was unreasonable because agents had no suggestion that the defendant's *particular acts* of sex trafficking had any transnational link. *Id.* at 721. Agents must not only figure out which *types* of crimes have the "transnational" nature that will justify searches, but they must also figure out whether *specific instances* of those crimes are sufficiently "transnational" in application.

Border officials process 1.1 million passengers and pedestrians *every single day*. CBP, *Snapshot*. These difficult determinations will arise frequently. And to process over one million entrants daily, agents must make such determinations quickly, lest the orderly flow of America's ports of entry completely break down. Thus, this Court has noted that "complex" doctrinal tests "have no place" at the border. *See Flores-Montano*, 541 U.S. at 152. Border officials need clarity; *Cano* and *Aigbekaen* do not provide it.

CONCLUSION

For the foregoing reasons, the United States respectfully requests that this Court vacate the decision of the panel below and remand with instructions to apply the *Touset* standard that requires no particularized suspicion for forensic border searches.

Alternatively, if this Court determines that reasonable suspicion is required, the United States respectfully requests that this Court affirm the judgment of the panel below that reasonable suspicion of any criminal activity will support a forensic border search.

Respectfully Submitted,

/s/ Matt Clarkston

Matt Clarkston
Counsel for Respondent
Dated: February 22, 2021

APPENDIX

CONSTITUTIONAL PROVISIONS

Fourth Amendment to the United States Constitution

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.

STATUTORY PROVISIONS

18 U.S.C. § 1001

(a) Except as otherwise provided in this section, whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully--

(1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact;

(2) makes any materially false, fictitious, or fraudulent statement or representation; or

(3) makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry;

shall be fined under this title, imprisoned not more than 5 years or, if the offense involves international or domestic terrorism (as defined in section 2331), imprisoned not more than 8 years, or both. If the matter relates to an offense under chapter 109A, 109B, 110, or 117, or section 1591, then the term of imprisonment imposed under this section shall be not more than 8 years.

(b) Subsection (a) does not apply to a party to a judicial proceeding, or that party's counsel, for statements, representations, writings or documents submitted by such party or counsel to a judge or magistrate in that proceeding.

(c) With respect to any matter within the jurisdiction of the legislative branch, subsection (a) shall apply only to--

(1) administrative matters, including a claim for payment, a matter related to the procurement of property or services, personnel or employment practices, or support services, or a document required by law, rule, or regulation to be submitted to the Congress or any office or officer within the legislative branch; or

(2) any investigation or review, conducted pursuant to the authority of any committee, subcommittee, commission or office of the Congress, consistent with applicable rules of the House or Senate.