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 PETITIONER

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

QUESTION PRESENTED

1. Do warrantless forensic searches of digital devices at the border require reasonable suspicion under the Fourth Amendment?
2. What must officials reasonably suspect to find in a digital device for a warrantless forensic digital search to be permissible under the Fourth Amendment?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTRODUCTION

Digital devices like cell phones and laptops contain troves of intimate personal information. But at the border, the Government views digital devices as mere luggage that can be rummaged through without a warrant or suspicion. Petitioner Derrick Williams, Jr. learned this the hard way when he returned home to the United States from a trip abroad. Despite no evidence hinting that Williams's devices contained contraband, a band of Homeland Security agents seized his laptop and combed through his hard drive in a forensic search. Williams now faces criminal charges based on evidence obtained in a search that violated his fundamental Fourth Amendment rights. The Government claims its authority to protect the border authorized the search of William's laptop. Its interpretation of the Fourth Amendment is simple: at the border, anything goes.

This Court should reject this dangerous position. Searches of digital data present unparalleled privacy concerns and are only tenuously tethered to this Court's rationale for permitting warrantless border searches. This Court should hold that warrantless, forensic searches of digital devices at the border are only permissible when officials reasonably suspect a device contains contraband.

STATEMENT OF THE CASE

I. Factual Background

A. A Lone Homeland Security Agent Flags Derrick Williams as a Person of Interest in a Terrorist Attack Despite Finding No Evidence Linking Williams to the Attack.

In August 2015, United States officials were notified that an American citizen had been arrested in Germany. R. at 15. A Federal Bureau of Investigations

(FBI) field office then sent a letter to Homeland Security Special Agent Kyle Allen. R. at 15. The letter explained that Derrick Williams, Jr. was arrested for possessing a bow and arrow and air gun in violation of German law. R. at 15. At the time of his arrest, Williams provided German officials his travel itinerary: a trip consisting of stops of in Iceland, Amsterdam, Germany, Belgium, and Morocco. R. at 15. The letter also stated that Williams was present in Germany from 2007 until 2011, when German officials discovered that his visa had expired in 2008. R. at 15. Because of the visa violation, German authorities put an alert on Williams and banned him from entering the Schengen Area[1] for five years. R. at 15.

The letter prompted Allen to check Williams's criminal history and passport application. R. at 16. He learned Williams had prior convictions for trespass, use of a financial instrument, and fraud in the United States. R. at 16. He also learned Williams earned an additional conviction for escape when he left the country during his community corrections sentence. R. at 16. Other than conducting this quick background check and obtaining a copy of Williams's passport application, Allen "apparently did little else with respect to Williams until November 2015." R. at 16.

But Allen came under pressure after a terrorist group claiming allegiance to the Islamic state gruesomely attacked civilians in Paris on November 13, 2015, and

---

[1] The Schengen Area is a group of European countries that permits travelers to freely cross their borders once a traveler is lawfully admitted into a member country. The Schengen Area covers most of the countries in the European Union, including Belgium, France, Germany, Iceland, and the Netherlands. *See* https://www.schengenvisainfo.com/schengen-visa-countries-list/.

authorities searched desperately for the suspects. R. at 8, 16. Allen's supervisors demanded that he review his current investigations and identify persons "of interest." R. at 16. Allen had no information linking Williams to the attacks, but he nonetheless put a "lookout" alert on Williams in the Customs and Border Patrol (CBP) database. R. at 16-17. The alert instructed CBP officials to detain Williams for secondary questioning when he returned to the United States. R. at 17. Williams is recognizably Muslim. R. at 19.

B. A Team of Agents Interrogates Williams and Finds No Link to the Terrorist Attack.

Six days later, Allen received an alert that Williams had boarded a flight from Paris to Denver. R. at 17. Allen came prepared: at his request, "two Homeland Security computer forensic agents also arranged to be there, in case Williams was carrying electronic devices that could not be searched without special tools." R. at 17.

Williams disembarked at Denver and gave his customs declaration form to a CBP officer, who then passed the form to Allen. R. at 17. Allen noted the permanent address on the form matched the address on Williams's passport application. R. at 17. But he also saw that Williams omitted Germany from the "countries visited on this trip prior to U.S. arrival" section of the form. R. at 17-18.

After answering questions from multiple CBP officers in two separate inspection areas, Williams was finally brought to another interview room where he fielded thirty minutes of questions from Allen and a local police detective who was part of an FBI joint counterterrorism task force. R. at 18. They demanded to know

why Williams had spent six months abroad. R. at 18. Williams explained that he was engaged to marry a woman in Morocco and that he had spent the time visiting her and completing the marriage approval process. R. at 18-19. Williams had stayed with a Muslim friend in Belgium when his Moroccan visitor visa expired to avoid an expensive return flight to the United States. R. at 19. He then returned to Morocco and married his fiancé. R. at 19. Williams avoided answering when Allen and the detective repeatedly asked whether he had visited Germany. R. at 20. He admitted that he lived in Germany on an expired visa years earlier after he ran out of money to return to the United States, and that he had been banned after the discovery of his visa violation. R. at 21. After Allen and the detective continued to question him about Germany, Williams quipped that the fatigue of travel and aging was affecting his memory. R at 21. He told his interrogators to look in his passport and check with the consulate in Morocco to confirm his travels. R. at 20-21. He felt the agents were being dishonest by asking him questions to which they already knew the answers. R. at 21.

Allen and the detective commanded Williams to share his laptop and smartphone passwords. R. at 20. Williams refused because he believed a search of his devices would be an invasion of his constitutional rights. R. 20. He accused the agents of targeting him because he was Muslim. R. at 20.

C. After Releasing Williams, Agents Conduct a Warrantless Forensic Search of His Laptop.

While Allen and the detective interrogated Williams, CBP officers rifled through his luggage and "found nothing of immediate concern." R. at 18. They tried

to break into his laptop and smartphones, but could not crack the standard password protection on the devices. R. at 18. The computer forensic agents Allen brought to the airport "went to work" and used their "light-weight forensic equipment" to try to get around the passwords but to no avail. R. at 18.

Allen eventually released Williams to go home with his luggage but kept his laptop and smartphone. R. at 21. The next morning, Allen took the devices to a Homeland Security office for further investigation. R. at 21. The computer forensic agents removed the laptop's hard drive and made a "bit-for-bit copy" so they could "work on" and inspect the copy without altering the original. R. at 22.

Five days later, one of the Homeland Security computer agents who tried to crack the passwords at the airport conducted a forensic digital search of Williams's laptop. R. at 22. The agent uploaded the copy of the hard drive to Encase, "a computer program used for forensic examination of digital media." R. at 22. After the program processed all of Williams's laptop data and recovered deleted or "lost" folders, it displayed the contents of his hard drive in its user interface. R. at 22-23. The agent perused the files and noticed a folder titled "Issue 15 little Duchess." R. at 23. He opened that folder and discovered child pornography. R. at 23. He alerted Allen, who finally applied for a search warrant to examine the entire laptop. R. at 23. A judge issued the warrant on December 4, 2015: three days after agents loaded Williams's hard drive into a forensic search program, and nine days after they seized his digital devices at the border. R. at 23.

Six months later, the computer agent completed his report on Williams's laptop. R. at 24. He discovered images and videos "consistent with child pornography." R. at 24.The forensic search of the smartphone dragged even longer—the agents could not crack the passcode with their forensic equipment, and sent it to another lab for investigation. R. at 24. That lab finally accessed the phone's data "several months later" but did not find any contraband files. R. at 24.

II. Procedural History

A. A Grand Jury Indicts Williams Based on Evidence Taken From His Laptop.

Only July 27, 2016, a grand jury indicted Williams with the offenses of transportation and possession of child pornography. R. at 24. He was arrested on September 26, 2016. R. at 24.

B. The District Court Denies Williams's Motion to Suppress the Evidence Obtained in the Warrantless Search of His Laptop.

Williams moved to suppress the evidence derived from the search of his laptop as a violation of his Fourth Amendment rights. R. at 37. The District Court of Colorado denied the motion. R. at 37.

After surveying this Court's border search jurisprudence, the district court concluded the Government could "conduct some searches at the border entirely without suspicion of criminal wrongdoing, while some other set of searches must be justified by reasonable suspicion." R. at 29-30. And if reasonable suspicion exists, "intrusive measures" are permissible. R. at 30. The court noted that most of the decisions upholding suspicionless searches "predate the point when smartphone ownership became nearly ubiquitous." R. at 30-31. More recent decisions

"[r]ecognizing that digital devices can (and usually do) hold the equivalent of warehouses worth of private information about their owners, and that cloud computing may augment this by many orders of magnitude" have found some searches of digital devices to be highly intrusive and thus demand suspicion. R. at 31. It noted that these courts have "largely settled" on the rule that a "manual" digital search requires no suspicion, while "a forensic search that creates an easily searchable image of all data on the device, potentially including deleted data, and which can be preserved and examined at the Government's leisure" requires reasonable suspicion.[2] R. at 31; *United States v. Cotterman*, 709 F.3d 952, 960–66 (9th Cir. 2013) (en banc).

But the district court declined to rule on the appropriate legal standard. R. at 31. It did not decide whether forensic digital searches fell into the suspicionless category or the reasonable suspicion category. R. at 31. Nor did it decide whether the search of Williams's laptop was a manual or forensic search. R. at 31-32. The court concluded that under either rule and either kind of search, the search of Williams's laptop was permissible because the Homeland Security agents reasonably suspected him to be engaged in criminal activity. R. at 32.

---

[2] The district court defined a "manual" search as "examining a non-password-protected device by browsing through immediately available directories and files, akin to rummaging through luggage, and a "forensic" search as a "search that creates an easily searchable image of all data on the device, potentially including deleted data, and which can be preserved and examined at the Government's leisure." R. at 30.

The district court found the agents had a "particularized and objective basis" to suspect Williams's devices contained evidence of criminal activity. R. at 32, 35 (quoting *United States v. Mabry*, 728 F.3d 1163, 1167 (10th Cir. 2013)). First, Allen knew Williams made a false statement on his customs declaration form by omitting Germany, which is a violation of 18 U.S.C. § 1001. R. at 34. Second, Williams refused to confirm that he had visited Germany during his interrogation. R. at 35. And lastly, the agents had reason to suspect Williams was "attempting to distance himself from his digital devices" solely because he listed a different address on the claim forms for his devices than the permanent address on his passport application and customs declaration. R. at 35. The court was satisfied that a reasonable officer could "conclude that Williams's digital devices contained evidence of an ongoing crime, such as materials whose importation into or possession in the United States would be a violation of customs or other laws." R. at 35.

C. The Tenth Circuit Court of Appeals Affirms the District Court and Holds Reasonable Suspicion of General Criminal Activity Justifies a Warrantless Forensic Search of a Digital Device at the Border.

Williams appealed and argued the district court erred in holding the search of his laptop was supported by reasonable suspicion, and that the warrantless search of his laptop violated the Fourth Amendment. R. at 10. The Tenth Circuit affirmed the district court. R. at 11.

Reviewing the question of the legal standard for a digital search conducted at the border de novo, the Tenth Circuit held a reasonable suspicion of *any* criminal activity is "sufficient to justify a border search of personal electronic devices,"

regardless of whether the suspected activity has anything to do with a border-related offense. R. at 11.

The Tenth Circuit agreed with the lower court that the officers had reason to suspect Williams of criminal activity. R. at 11. Under the totality of circumstances—Williams's criminal convictions, his omission on the customs form, his evasive answers to Allen, his travel to a country that had recently suffered a terrorist attack, and the additional address he wrote on his claim forms—"a warrantless search of the laptop and cell phone" were justified. R. at 11-13. The court did not specify exactly what crime the agents were justified in suspecting Williams to be engaged in. R. at 13. It concluded the type of crime the agents suspected was irrelevant R. at 13.

Seeking to overturn the Tenth Circuit's decision, Williams sought a writ of certiorari on the question of the appropriate legal standard for a forensic digital search at the border. This Court granted the petition.

SUMMARY OF ARGUMENTS

The Tenth Circuit erred in holding that reasonable suspicion of any criminal activity justifies a warrantless forensic search of a digital device at the border. This Court should reverse the Tenth Circuit and hold that absent a warrant, forensic digital searches are only permissible under the Fourth Amendment when officials reasonably suspect a device contains contraband. This standard balances the Government's legitimate interests in conducting warrantless border searches to interdict contraband against the significant privacy and dignity concerns unique to

digital data. And because the agents here had no reason to suspect that Williams's laptop contained digital contraband, this Court should reverse the lower court and grant Williams's motion to suppress the evidence illegally obtained from his hard drive.

First, forensic digital searches require reasonable suspicion. This Court has held that non-routine border searches require heightened justification, and forensic searches of digital devices are non-routine because they are highly invasive and infringe personal privacy and dignity. The forensic examination of Williams hard drive was a non-routine search that demanded reasonable suspicion.

Second, border officials must reasonably suspect a digital device contains contraband—not merely evidence of criminal activity. The history of the border search exception and this Court's precedents illustrate that warrantless border searches are only permissible when a search is necessary to prevent the unlawful entry of persons and contraband. And a search of a digital device is tethered to this purpose only when officers reasonably suspect a device to contain digital contraband.

A digital contraband standard protects individual privacy and the nation's borders. It enables border officials to apprehend suspected smugglers of child pornography while maintaining consistency with this Court's rule principle that intrusive searches demand heightened justification. And a digital contraband standard avoids inviting the racial profiling that is likely to occur under a "general suspicion" or even a "border-nexus" standard. Finally, the standard does not

undermine protection of the United States border because officials can still conduct forensic digital searches by obtaining a warrant or invoking the exigent circumstances doctrine in emergencies.

Because the agents here had no reason to think Williams's digital devices contained contraband, the Government did not have a legitimate purpose in conducting the warrantless, forensic search of his laptop. And even such a search was justified by reasonable suspicion that a device contained evidence of a crime with a border-nexus, there was no basis to suspect Williams's laptop contained evidence of transnational crime. This Court should reverse the Tenth Circuit and hold that warrantless forensic searches of digital devices are only permissible when officials reasonably suspect a device contains digital contraband.

ARGUMENT

I. The Fourth Amendment Prohibits Unreasonable Searches and Seizures.

"The Fourth Amendment commands that searches and seizures be reasonable." *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985). The desire for freedom from "unrestrained search[es] for evidence of criminal activity" was "one of the driving forces behind the Revolution itself." *Riley v. California*, 573 U.S. 373, 403 (2014).

This Court has created a balancing test to determine whether a search is reasonable under the Fourth Amendment. *Id.* 403. Courts must balance "the degree to which [a search] intrudes upon an individual's privacy, and on the other, the degree to which it is needed for the promotion of legitimate government interests." *Id.* (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)). To satisfy this

balancing test, law enforcement typically need only follow a simple procedure before conducting a search: "get a warrant." *Id.*

Searches conducted without a warrant are "per se unreasonable under the Fourth Amendment." *Katz v. United States,* 389 U.S. 347, 357 (1967). The process of obtaining a warrant from a neutral decision-maker guarantees that the government's interests in conducting the search are fairly evaluated and balanced against the individual privacy interests at stake. *Johnson v. United States*, 333 U.S. 10, 14 (1948). Warrantless searches circumvent this important check on law enforcement discretion. A warrantless search is thus only reasonable if the Government can demonstrate that one the few "specifically established and well-delineated exceptions" to the warrant requirement applies. *Katz*, 389 U.S. at 357.

The border search exception is one of the well-delineated exceptions to the warrant requirement. The long-standing border search exception permits the Government to conduct warrantless and suspicionless routine searches at the United States border to prevent the illegal entry of persons and contraband. *United States v. Ramsey,* 431 U.S. 606, 616-17 (1977); *Montoya de Hernandez*, 473 U.S. at 357.

But the border search exception is not boundless. Border searches are subject to two key limitations. First, this Court has held that highly intrusive searches that infringe the personal privacy and dignity of the traveler are non-routine and require reasonable suspicion. *Montoya de Hernandez*, 473 U.S. at 544; *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004). Second, as this Court has affirmed

"[t]ime and time again," the border search exception exists to prevent the illegal entry of persons and contraband. *Flores-Montano*, 541 U.S. at 152-53; *Ramsey*, 431 U.S. at 616; *Montoya de Hernandez*, 473 U.S. at 538-39. This Court has never held that the border search exception exists to detect evidence of criminal activity or promote general law enforcement.

II. The Warrantless Forensic Search of Williams's Digital Device was Unconstitutional Because the Government Did Not Suspect the Device Contained Digital Contraband.

The warrantless search of Williams's laptop was not justified by the border search exception. *See* R. at 22-23. This Court's recent decision in *Riley* addresses both issues presented by this case: how searches of digital devices infringe personal privacy and how warrant exceptions apply to digital searches. *Riley*, 573 U.S. at 386, 393-97. First, as this Court recognized in *Riley*, the vast amount of intimate information stored on digital devices implicates significant privacy interests. 573 U.S. at 393-97. And because forensic digital searches give the Government unbridled access to this private information, they are non-routine border searches that require particularized suspicion. *See Montoya de Hernandez*, 473 U.S. at 544; *Flores-Montano*, 541 U.S. at 152; *Cotterman*, 709 F.3d at 957 (describing forensic digital examinations). Second, forensically examining the private information stored on a digital device only connects to this Court's rationales for warrantless border searches—preventing the entry of unwanted persons and effects—if officials suspect that digital contraband is stored within a device. *United States v. Cano*, 934 F.3d 1002, 1007 (9th Cir. 2019) (en banc rehearing denied).

This Court should reverse the Tenth Circuit and hold that warrantless forensic searches of digital devices at the border are only permissible when officials reasonably suspect that a device contains contraband. *See id*. A digital contraband strikes a crucial balance between protecting individual privacy and protecting the border. Because there was no basis to suspect Williams's hard drive contained contraband, the warrantless forensic search of his laptop was unreasonable and unconstitutional. *See* R. at 22-23.

A. The Search of Williams's Laptop Required Reasonable Suspicion.

1. Highly intrusive border searches that infringe personal privacy and dignity are non-routine and require reasonable suspicion.

This Court has long distinguished routine border searches that may be conducted without suspicion from non-routine searches that require heightened justification. *Montoya de Hernandez*; 473 U.S at 538, 541; *Flores-Montano,* 541 U.S. at 152. The border search exception recognizes that some warrantless searches are necessary to prevent "unwanted persons and effects" from entering the country. *See Flores-Montano*, 473 U.S. at 152. That is why "routine searches of the persons and effects of entrants"—rifling through luggage, scanning travelers' clothing, inspecting automobiles, opening envelopes, and the like—are per se reasonable and not "not subject to any requirement of reasonable suspicion, probable cause, or warrant. *Montoya de Hernandez*, 473 U.S. at 538.; *see e.g., Flores-Montano*, 473 U.S. at 155-156 (upholding a warrantless and suspicionless vehicle inspection at the border); *Ramsey*, 431 U.S. at 624-625 (upholding warrantless border searches of international mail).

But this Court has held that "highly intrusive" border searches that infringe "dignity and privacy interests" are non-routine and demand reasonable suspicion. *See Flores-Montano,* 541 U.S. at 152; *Montoya de Hernandez*; 473 U.S at 541. In *Montoya de Hernandez*, this Court held that the strip search and lengthy detention of a traveler suspected of smuggling drugs was non-routine and required reasonable suspicion. 473 U.S. at 541. This Court explained that the "long, uncomfortable, indeed, humiliating" search was distinct from the "*routine* searches of the persons and effects of entrants" that do not require suspicion. *Id.* at 538, 544 (emphasis added). By contrast, the non-routine search of de Hernandez was only acceptable because border officials "reasonably suspected she was smuggling drugs in her alimentary canal." *Id.* at 535, 541. This Court counted "strip, body-cavity, or involuntary x-rays" are other non-routine border searches that demand suspicion. *Id.* at 541 n. 4.

On the other hand, this Court held that the disassembly of an automobile's fuel tank at the border was a routine border search because the concerns of personal privacy and dignity "simply do not carry over to vehicles." *Flores-Montano*, 541 U.S. at 150, 152.

Courts apply the *Montoya de Hernandez* and *Flores-Montano* framework to determine whether a particular border search requires reasonable suspicion. They consider the intrusiveness and degree of privacy and dignity implicated by a particular search to determine whether it is non-routine and requires reasonable suspicion. *See, e.g., Cotterman*, 709 F.3d at 962-68 (holding that forensic searches of

digital devices are non-routine and require reasonable suspicion because "such a thorough and detailed search of the most intimate details of one's life is a substantial intrusion upon personal privacy and dignity").

2. The examination of Williams's digital data invaded his personal privacy and dignity.

While concerns of personal privacy and dignity may not carry over to vehicle inspections, they certainly carry over to searches of digital devices. *See Flores-Montano,* 541 U.S. at 1532. This Court has recognized that the sensitivity and enormous breadth of information stored on personal digital devices raise privacy concerns unlike any other physical property. *Riley,* 573 U.S. at 403; *see also Carpenter v. United States*, 138 S. Ct. 2206, 2221 (2018) (holding that the Government must obtain a warrant before accessing historical cell-site records due to the significant privacy interests implicated by digital data). In *Riley*, this Court held that the incident to arrest exception[3] did not justify warrantless searches of cell phones. 573 U.S. at 393-397, 403. It dismissed the Government's argument that cell phones are materially indistinguishable from other physical possessions as "like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Id.* at 393. Rather, it found that a search through the troves of personal

[3] The "incident to arrest" exception permits warrantless searches of the person of an arrestee when necessary to protect officer safety and prevent the destruction of evidence. *Chimel v. California,* 395 U.S. 752, 762-63 (1969).

information stored on a cell phone "implicate[s] privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." *Id.* at 393-397.

The exhaustive examination of the personal information stored on Williams's laptop also implicated dignity and privacy concerns unmatched by searches of other physical property. *See id.*; R. at 22-23. Indeed, the privacy interests recognized in *Riley* apply with even greater force to searches of digital data at the border. *See id; see also Cotterman*, 709 F.3d at 962-68 (discussing digital privacy concerns in the context of border searches). "[A]n arrestee's reduced privacy interests upon being taken into police custody" are far more "diminished" than the privacy interests of an international traveler. *See id.* at 391; *Flores-Montano*, 541 U.S. at 154 ("[T]he expectation of privacy is less at the border than it is in the interior."). The arrestee has been physically restrained and taken into custody by law enforcement; the international traveler has merely "presented herself at the border for admission." *See Riley*, 573 U.S. at 393; *Montoya de Hernandez*, 473 U.S. at 539. The privacy interests identified by *Riley* are even more profound at the border.

First, *Riley* recognized that the "immense storage capacity" of digital devices presents privacy issues distinct from other physical property. *Riley*, 573 U.S. at 393-396. Digital devices are "capable of storing warehouses full of information." *Cotterman,* 709 F.3d at 964. From the broad array of information ("an address, a note, a prescription, a bank statement, a video"), to the depth of information ("a thousand photographs labeled with dates, locations and descriptions") to the time span of the information ("the data on a phone can date back to a purchase, or even

earlier"), this Court found the storage capacity of a cell phone presented multiple significant privacy concerns. *Riley*, 573 U.S. at 394. And the concerns apply to other digital devices with immense storage capacities. **I**ndeed, "the average 400-gigabyte laptop hard drive can store over 200 million pages—the equivalent of five floors of a typical academic library." *Cotterman*, 709 F.3d at 964.

Second, *Riley* stressed the personal nature of digital data. 573 U.S. at 395-96. Digital devices "contain the most intimate details of our lives." *Cotterman*, 709 F.3d at 965. They include family photographs, financial records, dating apps, confidential business documents, medical data, internet search histories, private messages, and much more. *See id*; *Riley* 573 U.S. at 395-96. This deeply personal information "form[s] a revealing montage of the user's life" and "stands in stark contrast to the generic and impersonal contents of a gas tank." *Riley*, 573 U.S. at 396; *Cotterman,* 709 F.3d. at 964. Williams understandably had a significant privacy interest in withholding his passwords to prevent the Government from obtaining unfettered access to the virtual library of his private life. R. at 20.

Riley also noted that cloud computing compounds these privacy concerns. 573 U.S. at 397. If a device is connected to the cloud, a search of a device can reveal data that "may not in fact be stored on the device itself." *Id*. This Court described accessing remote files in a search as akin to "finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house." *Id*. If Williams's laptop was connected to the cloud, the forensic search of his hard drive would have given the border agents access to information that was not even on his

person when he crossed the border. *See id.*; R. at 20. No other search of physical property risks revealing information and property beyond the travelers' immediate effects. *Riley*, 573 U.S. at 398 (concluding the same for other searches incident to arrest).

A forensic digital search exhaustively exposes the vast collection of private information on a digital device. Forensic digital examination "is a powerful tool capable of unlocking password-protected files, restoring deleted material, and retrieving images viewed on websites." *Cotterman,* F.3d at 957. Forensic searches typically use external equipment and specialized software to retrieve data. *United States v. Kolsuz*, 890 F.3d 133, 146 n.6. (4th Cir. 2018). And unlike physical searches of luggage, forensic digital searches can drag on for months—"the only limit is the time the analyst has to give to the case." *See* Orin Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 569 (2005). The invasive and lengthy procedure is nothing like scanning a suitcase, inspecting a vehicle, or opening an envelope. *Cf. Ramsey*, 431 U.S. at 624-25. A forensic digital examination is essentially a "computer strip search." *Cotterman*, 709 F.3d at 966.

When the agents conducted the warrantless forensic examination of Williams's laptop, they forced entry to the library of his most private information. R. at 22-23. Given the immense amount of sensitive information accessible in a digital search, the examination of his laptop was nothing like the impersonal and technical disassembly of a fuel tank in *Flores-Montano. See* 541 U.S. at 152; R. at 22-23. Rather, Williams experienced an invasion of privacy and dignity as acute and

as "humiliating" as the strip-searched traveler in *Montoya de Hernandez*. *See* 473 U.S. at 544; R. at 22-23.

3. The forensic search of Williams's laptop was a non-routine search that required reasonable suspicion.

Given the significant privacy and dignity concerns raised by forensic digital searches, the majority of circuit courts that have addressed the issue agree that such searches are non-routine and require heightened justification. *See, e.g., Cano*, 934 F.3d at 1007 (the Ninth Circuit); *United States v. Aigbekaen*, 943 F.3d 713, 721 (4th Cir. 2019).

Only one circuit has held that forensic digital examinations are routine border searches and may be conducted without suspicion. *United States v. Touset*, 890 F.3d 1227, 1243 (11th Cir. 2018). The Eleventh Circuit reasoned that because this Court has never labeled any border search of property non-routine, only searches of the person can be non-routine and require suspicion. *Id.* This reasoning disregards this Court's decision in *Riley* and overlooks the fact that this Court has only considered two searches since it announced the routine and non-routine distinction: the strip search in *Montoya de Hernandez* and the vehicle search in *Flores-Montano*. *Montoya de Hernandez*, 473 U.S. at 534; *Flores-Montano*, 541 U.S. at 151. Both of those decisions predate the ubiquity of personal digital devices and this Court's recognition in *Riley* that digital searches present privacy concerns unlike any other search of physical property. *See Montoya de Hernandez*, 473 U.S. at 534 (decided in 1985); *Flores-Montano*, 541 U.S. at 151 (decided in 2004); *Riley*, 573 U.S. at 403 (2014). And neither decision rested on a distinction between persons

and property. *Montoya de Hernandez*, 473 U.S. at 541; *Flores-Montano*, 541 U.S. at 152. Rather, they turned on whether the particular search implicated personal privacy and dignity interests. *Id*. The Eleventh Circuit's property versus person distinction is misplaced and does not negate the significant privacy concerns implicated by searches of digital devices. *Touset*, 890 F.3d at 1234.

The Eleventh Circuit also suggested that travelers who do not want the Government to access their personal data should simply leave their laptops and cell phones at home. *See id.* at 1233, 1235 ("[Travelers] are free to leave any property they do not want searched—unlike their bodies—at home"). This advice assumes that travelers can control the data stored on their devices and that travelling without a digital device is a practical option in the modern world. Neither assumption is based in reality.

For starters, many users are unaware of how much personal data their devices passively record. For example, most cell phones automatically track the user's location and can "reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." *Riley*, 573 U.S. at 396. Digital devices also generate and store metadata: "a wealth of information" about how the device and its contents have been used. Kerr, supra, at 542 (describing how operating systems automatically record "where files are located, who created them, and which users have rights to them" and how browsers track "the user's interests, habits, identity and online whereabouts, often unbeknownst to the user").

To make matters more difficult, there is little individuals can do to control the information on their digital devices It would be impractical for travelers to remove a massive volume of "intermingled" files and metadata before every international trip. *See Cotterman*, 709 F.3d at 965. And even if a travler spend hours trying to remove their data, the effort likely would be for naught. Digital devices store data "far beyond the perceived point of erasure," and forensic searches can recover ostensibly deleted information and browsing histories. *Id.* at 964-65. Individuals cannot simply choose what personal information to leave behind when they travel with digital devices.

Nor can individuals afford to travel without their digital devices. Digital devices are a "pervasive and insistent part of daily life," and maintaining connectivity through these devices while travelling has become not just a convenience, but a responsibility. *See Riley*, 573 U.S. at 385. Leaving behind a cell phone or laptop disconnects a professional from their client, a student from their schoolwork, a parent from their child, or in this case, Williams from his fiancé in Morocco. *See* R. at 19. Travelling without digital devices is simply not an option.

Digital devices thus present a catch-22 situation for international travelers. On one hand, they cannot afford to disconnect and travel without their digital devices. But if they bring the devices along, they run the risk of border officials forensically examining their most intimate information. "[T]he ultimate touchstone of the Fourth Amendment is reasonableness," and it would be patently unreasonable for border officials to take advantage of travelers' dependence on

digital devices and pry into their private lives without suspicion. *See Brigham City v. Stuart*, 547 U.S. 398, 403 (2006). Because of the weighty privacy and dignity interests implicated by searches of digital devices, this Court should hold that forensic searches of digital devices are non-routine border searches that require reasonable suspicion.

B. The Search of Williams's Laptop Fell Outside the Scope of the Border Search Exception Because the Agents Had No Reason to Suspect the Laptop Contained Contraband.

This Court has repeatedly affirmed that "the [s]cope of the search must be strictly tied to and justified by the circumstances which rendered its initiation permissible." *Terry v. Ohio*, 392 U.S. 1, 19 (1968) (citations omitted). The Government can only invoke an exception to the warrant requirement if its interest in conducting the warrantless search links to the purpose of the exception. *See Riley*, 573 U.S. at 386.

The purpose of the border search exception is to prevent the entry of illegal persons and contraband. *Flores-Montano*, 541 U.S. at 152-153. This purpose is evident from history and reinforced by this Court's border search jurisprudence. *See id.* Though forensic digital devices contain vast amounts of information, their files cannot contain physical contraband. *Cano*, 934 F.3d at 1013-14. Only *digital contraband* links to the purpose of warrantless border searches. *Id.* Forensic digital searches are thus tethered to the justifications underlying the border search exception only when officials reasonably suspect a device contains digital contraband—not merely evidence of contraband, evidence of a transnational crime, or evidence of general criminal activity. *Id.* at 1020. Because the agents who

searched Williams's laptop had no reason to suspect his hard drive contained contraband, the search fell outside the scope of the warrant exception and was unreasonable. *See* R. at 22-23.

1. The purpose of a warrant exception limits the scope of the exception.

The governmental interests underlying a warrant exception "define the boundaries of the exception." *Arizona v. Gant*, 556 U.S. 332, 339 (2009). The few exceptions to the warrant requirement recognize narrow circumstances where courts may presume searches are reasonable under the Fourth Amendment; that is, circumstances where the government's legitimate interests in conducting a search balance against the privacy concerns implicated by the search. *See Riley*, 573 U.S. at 385. This Court has created a test to determine whether a warrant exception applies. *Id.* at 386. Rather than automatically extending warrant exceptions developed in earlier precedents, courts consider whether applying an exception to a "particular category of effects" would "untether the rule" from its underlying justifications. *Id.* If the search has no relation to the purpose of the exception, the warrantless search is unreasonable. *Id.*

This Court applied this test in *Riley* before to hold the incident to arrest exception did not justify warrantless searches of cell phones seized from arrestees. *Id.* at 401. This Court found that allowing police officers to seize arrestees' phones and skim through their call histories, messages, and photos without warrant did not further either of the governmental interests at the core of the incident to arrest exception: protecting officer safety and preserving evidence. *Id.* at 378-80, 387, 389-

91. The data on the phones posed no threat of physical harm to an officer. *Id*. at 387. Nor was there any risk of evidence destruction because arrestees had no way to conceal or erase their cell phone data once the phones were secured by police. *Id.* at 389-91. Finding that cell phone searches were unconnected to the purpose of the incident to arrest exception, this Court held warrantless searches of cell phones seized incident to arrest were unreasonable. *Id.* at 401.

2. The purpose of the border search exception is to prevent the illegal entry of persons and contraband.

Applying *Riley*'s test here reveals that the "tether" between forensic digital searches and the rationale for the border search exception is tenuous. *See id.* at 386. Just as the incident to arrest exception does not permit "ransacking [a man's] house for everything which may incriminate him," the border search exception does not permit ransacking travelers' hard drives for incriminating data. *See id*. at 396 (quoting *United States v. Kirschenblatt,* 16 F.2d 202, 203 (2d. Cir. 1926)). This Court has repeatedly affirmed that the Fourth Amendment permits warrantless border searches "to prevent the introduction of contraband into this country." *Montoya de Hernandez*, 473 U.S. at 537. The forensic examination of Williams's laptop was untethered from this purpose because officials had no basis to suspect his hard drive contained contraband.

Detection of contraband is the strongest historic rationale for the border search exception. Two months before it proposed the Fourth Amendment to the states, the First Congress authorized customs officials to search "any ship or vessel, in which they shall have *reason to suspect* any *goods, wares, or merchandise* subject

to duty shall be concealed." *See Ramsey*, 431 U.S. at 616 (quoting the Act of July 31, 1789 C. 5, 1 Stat. 2 ("Customs Act")) (emphasis added). The Customs Act did not grant customs officers any authority "to obtain evidence of crimes other than the contraband itself." *United States v. Molina-Isidoro*, 884 F.3d 287, 295 (5th Cir. 2018) (Costa, J., concurring). And that limitation on the customs authority makes sense: authorizing customs officials to search for evidence of crimes would be a grant of a broad law enforcement power directly in conflict with the Fourth Amendment's prohibition against uncontrolled searches and seizures. As this Court explained in *Boyd v. United States*, the First Congress clearly regarded the contraband searches conducted by customs officials as reasonable under the Fourth Amendment. 116 U.S. 16, 623 (1886) (overruled in part on other grounds by *Warden, M.d. Penitentiary v. Hayden*, 387 U.S. 294 (1967)).[4] Though the Customs Act bestowed a "plenary" customs power, that power was only within the sphere of rooting out contraband. The customs power was not and is still not a plenary law enforcement power to search for evidence of criminal activity.[5] *See Ramsey*, 431 U.S. at 631.

---

[4] "The seizure of *stolen goods* is authorized by the common law; and the seizure of *goods forfeited for a breach of the revenue laws*, or *concealed to avoid the duties payable on them*, has been authorized by English statutes for at least two centuries past; and the like seizures have been authorized by our own revenue acts from the commencement of the government." *Boyd*, 116 U.S. at 623 (emphasis added).

[5] The modern customs statute has not expanded the authority of customs officers. The modern version of the statute authorizes border officials to seize only "*merchandise* which… shall have been introduced into the United States in any manner contrary to the law." 19 U.S.C. § 482(a) (emphasis added).

This Court's border search jurisprudence reinforces that the border exception exists to interdict contraband. This Court has reaffirmed in every border search case that the exception applies to searches for unlawful persons and goods. *See Boyd*, 116 U.S. at 623; *Carroll v. United States*, 267 U.S. 132, 154 (1925) (describing border searches as "reasonably requiring one entering the country to *identify himself as entitled to come in*, and his belongings *as effects which may lawfully be brought in*) (emphasis added); *Montoya de Hernandez*, 473 U.S. at 537 (describing the Executive's authority "to regulate the collection of duties and to *prevent the introduction of contraband* into this country") (emphasis added); *Flores-Montano,* 541 U.S. at 152 ("The Government's interest in preventing the entry of *unwanted persons and effects* is at its zenith at the international border.") (emphasis added).

Even *Ramsey*, this Court's broadest pronouncement of the Government's "sovereign" authority to conduct warrantless border searches, still grounded the purpose of border searches in preventing the entry of unwanted persons and objects. 431 U.S. at 620. Surveying border search history, this Court concluded warrantless border searches were "necessary *to prevent smuggling* and *to prevent prohibited articles* from entry." *Id.* at 619 (emphasis added). It also acknowledged that routine searches of travelers and their property effectuated the power to exclude aliens. *Id.* It concluded that the border search exception recognized the sovereign's right to control "*who and what* may enter the Country." *Id.* at 620 (emphasis added). Courts and commentators have recently questioned whether *Ramsey*'s sweeping analysis would still stand if this Court considered the recent historical work suggesting

border searches were originally limited to maritime customs searches. *See, e.g, Aigbekaen*, 943 F.3d at 728 (Harrison, J., concurring). But even *Ramsey* did not declare that warrantless border searches could extend to searches for evidence of general criminal activity. *See* 431 U.S. at 620.

Moreover, every border search case this Court has decided involved "searches to locate *items being smuggled* rather than evidence." *Molina-Isidoro*, 884 F.3d at 295 (Costa, J. concurring). In *Montoya de Hernandez*, the only instance where this Court addressed the suspicion required for a non-routine border search, the invasive search was justified because agents reasonably suspected the woman was "*smuggling contraband* in her alimentary canal." 473 U.S. at 541, (emphasis added). And in *Flores-Montano*, this Court found that the disassembly of an automobile fuel tank was well within the scope of the border search exception because of "evidence that *smugglers* frequently attempt to penetrate our borders with *contraband* secreted in their automobiles' fuel tank." 541 U.S. at 153 (emphasis added). This Court has never concluded that a warrantless border search was warranted solely to find evidence of general criminal activity. *Molina-Isidoro*, 884 F.3d at 295 (Costa, J. concurring).

Lastly, this Court has emphasized that the border search exception exists by virtue of the Government's interest in excluding persons and contraband. The border search exception is not "at all" based on the difficulty of obtaining a warrant at the border. *Ramsey,* 431 U.S. at 621. Rather, it recognizes that searches conducted for the specific purpose of apprehending contraband are exempt from the

warrant requirement, just like the incident to arrest exception recognizes searches conducted for the specific purposes of protecting officers or preserving evidence are exempt. *See id.; Riley*, 573 U.S. at 386. Warrantless border searches may also occur "not only at the border itself, but at its functional equivalents" when circumstances implicate the Government's interests in enforcing immigration and customs laws. *Almeida-Sanchez v. United States*, 413 U.S. 266, 273 (1973). This Court's precedents make it clear that officers may only invoke the border search exception when circumstances trigger the Government's interests in stopping unwanted persons and effects from entering the country.

History and this Court's decisions confirm that warrantless border searches are permissible only to prevent the illegal entry of persons and contraband. When a border search becomes "too attenuated from these historic rationales, it no longer will fall under the exception." *Aigbekaen*, 943 F.3d at 721 (citations omitted).

3. A forensic digital search is tethered to the purpose of the border search exception only if officials reasonably suspect the device contains contraband.

A search of a digital device links to the Government's interest in excluding persons and contraband only if officials suspect the device contains contraband files. *Cano*, 934 F.3d at 1007. This Court should therefore hold that absent a reasonable suspicion that a digital device contains contraband, a warrantless forensic digital search falls outside the scope of the border search exception and is unconstitutional.

First, digital contraband is the only type of digital data that bears any connection to the purpose of the border search exception. *Id.* at 1014, 1017. Forensically examining a digital device has nothing to do with preventing the entry

of inadmissible persons. *See Alasaad v. Nielsen,* 419 F. Supp. 3d 142, 158 (D. Mass. 2019). For American citizens like Williams, it is difficult to imagine what information his laptop could have contained that would have prevented his admission. *See* R. at 7. And even for non-citizens, it is unlikely that a forensic search could add anything to their case for admission that their customs form, visa application, passport, and travel history would not reveal. *See Alasaad,* 419 F. Supp. 3d at 158. Digital devices can, however, contain illegal files such as child pornography, classified information, or counterfeit media. *Cano*, 934 F.3d at 1014; *Alasaad*, 419 F. Supp. 3d at 158. Stopping travelers from carrying illegal files into the country goes directly to the anti-contraband rationale of the border search exception. *Cano*, 934 F.3d. at 1014.

Second, requiring reasonable suspicion of digital contraband is consistent with this Court's distinction between border searches for contraband and searches for evidence of criminal activity. *Id.* at 1017. The distinction is one "between seizing goods at the border because their importation is prohibited and seizing goods at the border because they may be useful in prosecuting crimes." *Id.* at 1018; *see also Boyd*, 116 U.S. at 622-23 ("The search for seizure of stolen or forfeited goods, or goods liable to duties and concealed to avoid the payment thereof, are totally different things from a search for and seizure of a man's private books and papers for the purpose of obtaining information therein contained, or of using them as evidence against him."). The dangers of searches for evidence of criminal activity are especially acute in the digital search context. Because of the sheer amount of

information on digital devices, most forensic digital searches reveal evidence of low-level crimes. Kerr, supra, at 570. Combing through a digital device for evidence of criminal activity is unfair to the user and untethered from the anti-contraband rationale that exempts border searches from the warrant requirement. Requiring suspicion of digital contraband ensures that warrantless forensic digital searches are conducted only when officials expect to find contraband, and not just evidence of criminal activity. *Cano*, 934 F.3d at 1017.

Third, a digital contraband standard effectively balances the private and public interests at stake in a digital border search. On one hand, requiring suspicion of digital contraband aligns with this Court's preference "to provide clear guidance to law enforcement through categorical rules" and imposes a "practical limit" on the discretion of border officials. *See Riley*, 573 U.S. at 398-99. This limit on the discretion is necessary to protect travelers from being subjected to extreme privacy violations based on the personal biases of border officials. Current CBP policy expressly permits border officials to rely on race and ethnicity as investigative or screening criteria "when a compelling governmental interest is present." U.S. Customs and Border Protection, *CBP Policy on Nondiscrimination in Law Enforcement Activities and all other Administered Programs,* https://www.cbp.gov/about/eeo-diversity/policies/nondiscrimination-law-enforcement-activities-and-all-other-administered# (last updated February 24, 2020). The result is that Muslim individuals like Williams are far more likely to be stopped, questioned, and searched at the border than other identity groups. *See* R.

at 20; *see, e.g.* N.Y. Times, *Traveling While Muslim Complicates Air Travel*, https://www.nytimes.com/2016/11/08/business/traveling-while-muslim-complicates-air-travel.html (Nov. 7, 2016). Requiring reasonable suspicion of digital contraband to authorize a warrantless forensic search of a digital device limits this discretion and protects travelers like Williams from discriminatory invasions of privacy.

At the same time that it curtails dangerous discretion, a digital contraband standard leaves officials with the authority to conduct powerful forensic searches to prevent illegal files from crossing the border. Signs of digital contraband are often readily apparent: border officials often detect suspicious activity related to the possession of child pornography before a traveler even arrives at the border. *See e.g., United States v. Wanjiku,* 919 F.3d 472, 477-78 (7th Cir. 2019); *Cotterman*, 709 F.3d at 957; *Touset*, 890 F.3d at 1230 (all describing investigations that flagged travelers as suspected carriers of child pornography well before they arrived at the border). And because routine border searches like luggage checks and interviews require no suspicion, officers can respond to the "emerging tableau" of circumstances and perform a forensic digital search if their initial routine searches provide a basis to suspect the individual's device contains contraband. *See Alasaad*, 419 F. Supp. 3d at 168 (quoting *United States v. Chhien*, 266 F.3d 1, 6 (1st Cir. 2001)).

And even when there is no basis to suspect a digital device contains contraband, border officials still have legal avenues to initiate forensic digital searches. One option is to secure a search warrant before the traveler arrives. In

Aigbekaen, for example, Homeland Security agents eventually secured warrants to search a sex trafficking suspect's digital devices based on evidence they possessed before he arrived at the border. *Id.* at 722**.** The Fourth Circuit concluded it was "only reasonable" to expect the Government to have secured the warrants before Aigbekaen's arrival. *Id.* at 722. Likewise, the agents who investigated Williams became aware of his arrest in Germany months before he returned to the United States and had ample time to secure a warrant to search his devices. *See* R. at 7.

And if there is no time to secure a warrant, the exigent circumstances doctrine provides a backstop. The doctrine permits officials to conduct warrantless searches when under the totality of circumstances "the exigencies of the situation make the needs of law enforcement so compelling that a warrantless search is objectively reasonable under the Fourth Amendment." *Missouri v. McNeely,* 569 U.S. 141, 148-49 (2013). This Court has recognized a variety of exigencies sufficient to justify a warrantless search, including the pursuit of a fleeing suspect and the prevention of imminent destruction of evidence. *Id*. If border officials faced a situation where they suspected a traveler's digital device contained information critical to protecting the border but they feared the evidence would be destroyed before they could obtain a warrant, they could invoke the exigent circumstances doctrine and conduct a warrantless search of the device. *See id.* Requiring suspicion of digital contraband in ordinary circumstances would not foreclose emergency forensic digital searches.

If there is no basis to suspect the traveler's digital devices contain contraband and no emergency, it is unreasonable for border officials to conduct a forensic digital search without a warrant. The digital contraband standard ensures that forensic digital searches further the purpose of the border search exception. This Court should reverse the Tenth Circuit and hold that border officials may only conduct a forensic digital search without a warrant when they have reason to suspect a device contains digital contraband.

4. Suspicion that a digital device contains merely evidence of criminal activity does not tether a forensic digital search to the purpose of the border search exception.

The two other reasonable suspicion standards articulated by the lower courts are insufficiently linked to the purpose of the border search exception and fail to balance private and public interests.

The lower court in this case held that reasonable suspicion of general criminal activity was sufficient to justify the warrantless forensic examination of Williams's laptop. R. at 13. This standard is completely untethered from the rationales that exempts border searches from the warrant requirement because the vast majority of criminal activity has nothing to do with immigration and customs violations. Under this standard, if officials reasonably suspect a traveler is engaged in a crime like financial fraud, border agents would have authority to forensically examine their digital devices for any and all incriminating evidence. The Tenth Circuit's standard is therefore inconsistent with the anti-contraband purpose of the border search doctrine and this Court's distinction between searches for contraband and searches for evidence of contraband. *See Boyd*, 116 U.S. at 622-23.

This standard also fails to guide border officials and invites pretextual searches. As evidenced by the lower court's conclusion that border officials had reason to suspect Williams of criminal activity, the threshold for suspicion is low. *See* R. at 11-13. Under the lower court's reasoning, any traveler with a criminal record and an omission on their customs form returning from a trip to a country linked to terrorist activity is fair game for a warrantless forensic digital search. *See* R. at 11-13. These criteria apply to millions of travelers and provide no protection to the significant privacy interests implicated by digital data. And if officials can invoke this standard to justify a search for any and all digital evidence of criminal activity, invasions of privacy are inevitable.

The Fourth Circuit has held that only reasonable suspicion of criminal activity with a "nexus" to the purposes of the border search exception justifies a warrantless forensic digital search. *See Aigbekaen*, 943 F.3d at 721. But this standard presents the same problems as the Tenth Circuit's rule. *See id.*; R. at 13. The Fourth Circuit has explained that a nexus to the purpose of the border search exception authorizes searches for *evidence* of past and future border related offenses. *Kolsuz*, 890 F.3d at 143. And it is the "interdiction of contraband, not the mere evidence of contraband" that triggers the Government's interest in protecting the border. *Alasaad,* 419 F. Supp. 3d at 156.

For starters, nearly any criminal activity can involve a "transnational component"—from international money laundering to a low-level conviction in a foreign country. *See Aigbekaen*, 943 F.3d at 721. The nexus standard thus would

authorize warrantless searches for evidence of these crimes that have nothing to do with protecting the border from contraband. *See id.* And like lower court's general suspicion of criminal activity standard, the vague requirement of a "border-search nexus" provides little guidance to border officials charged with screening the millions of travelers at the border. The Fourth Circuit's standard thus fails to balance providing the public interests animating the border search against the significant privacy concerns implicated by searches of digital data.

5. The forensic search of Williams's laptop was not justified by the border search exception because there was no basis to suspect the laptop contained contraband.

Reasonable suspicion requires more than an "inchoate and unparticularized suspicion or 'hunch'." *Terry*, 392 U.S. at 27. To determine whether a search was based on reasonable suspicion, courts consider the totality of the circumstances and ask whether the official conducting the search had a "particularized and objective" for suspecting the person of criminal activity. *United States v. Cortez*, 449 U.S. 411, 417-18 (1981).

Courts tends to focus on the traveler's criminal record and travel history to determine whether there was a reasonable basis to suspect a traveler possessed child pornography on their digital device. In *Cotterman*, for example, the defendant had been convicted of multiple sex offenses involving children and was also suspected of engaging in child sex tourism because of his frequent trips to Mexico. 709 F.3d at 957, 968-69. Cotterman's passport triggered an alert at the border, and officials conducted a warrantless forensic search of his laptop and discovered hidden, password-protected files that contained child pornography. *Id.* at 958-59.

The Ninth Circuit held the search was justified because Cotterman's criminal record and travel history gave officials reason to suspect his laptop contained child pornography. *Id.* at 971. And in *Wanjiku*, the defendant made multiple trips to the Philippines, another country associated with child sex tourism. 919 F.3d at 474-75. Wanjiku had a prior criminal history involving a minor, and an investigation of his social media profile revealed his friends were suspiciously younger than him. *Id.* at 475. Border officials put a lookout alert on Wanjiku, and he was interviewed and searched upon his return to the United States. *Id.* at 475-76. Officials found receipts for one-night hotel stays, syringes, condoms, and testosterone medication in his carry-on bag. *Id.* at 476-77. The officials then conducted warrantless forensic searches of his digital devices and discovered child pornography. *Id.* at 477-78. The Seventh Circuit concluded the agents had ample suspicion to conduct the searches. *Id.* at 488.

But the suspicion that a traveler possess child pornography must be particularized to be reasonable. The Fourth Circuit's decision in *Aigbekaen* demonstrates that just because a traveler is suspected of some criminal activity does not give border officials a basis to suspect digital contraband. 943 F.3d at 723. In *Aigbekaen*, border officials forensically searched the cell phone, laptop, and iPod of a man before obtaining a warrant. 943 F.3d at 717-18. Even though *Aigbekaen* was under investigation for sex trafficking a minor—a crime closely linked to the possession of child pornography—and even though police had some third-hand testimony suggesting he was involved in filming child pornography, the court found

the officials did not have a particularized basis to suspect his devices contained contraband. *Id.* at 721, 723-724.

Here, there was no particularized and objective basis for the Homeland Security agents to suspect that Williams's laptop contained child pornography. *See Cortez*, 449 U.S. at 417-18. Unlike Cotterman, Williams had no prior convictions for sex offenses, and no convictions for any conduct involving minors. *See Cotterman*, 709 F.3d at 971; R. at 16. Unlike Wanjiku, Williams had not visited countries known for child sex tourism and carried no suspicious items in his luggage. *See Wanjiku*, 919 F.3d at 988; R. at 18-19. If there was no reasonable basis to suspect a known child sex trafficker possessed child pornography on his digital devices, there was certainly no basis to suspect Williams possessed any digital contraband. *See Aigbekaen*, 943 F.3d at 723-724; R. at 16. Nothing in Williams criminal history, travel history, interview, or luggage suggested his laptop contained digital contraband. The warrantless forensic search of his laptop was therefore unconnected from the purpose of the border search exception and unreasonable. *See Cano*, 934 F.3d at 1020.

And even if suspicion that a device merely contained evidence of a border related crime was sufficient to justify a forensic digital search, there was no basis to suspect Williams's laptop contained any such evidence. In *Aigbekaen*, the Fourth Circuit determined that even though sex trafficking is frequently a transnational crime, the suspect's ongoing involvement in sex trafficking was purely domestic. 934 U.S. at 721**.** Officials thus had no reason to suspect a search of his devices would

reveal evidence of transnational criminal activity. *Id.* Likewise, there was no reason to suspect Williams's laptop contained evidence of a border-related crime. Nothing in Allen's investigation suggested Williams was engaged in any transnational criminal activity when he arrived in Denver. R. at 16. Like Aigbekaen, Williams's decade-old criminal history in the United States was completely domestic. *Aigbekaen*, 934 U.S. at 721; R. at 16. And unlike Aigbekaen, Williams was not the subject of an ongoing police investigation when he arrived at the border. *Aigbekaen*, 934 U.S. at 717-18; R. at 16. Again, if there was no reason to suspect Aigbekaen's digital devices contained evidence of a crime with a border search nexus, there was even less reason to think Williams's laptop contained this evidence. *Aigbekaen*, 934 U.S. at 717-18; R. at 16.

And even if the agents did have a basis to suspect that Williams was engaged in transnational criminal activity, there was no need for a forensic examination of his hard drive to confirm their suspicions. Allen was already aware that Williams overstayed his German visa years earlier and omitted his recent trip to Germany from his customs declaration form. R. at 16, 18. Allen did not need to obtain additional evidence for either of these offenses by searching Williams's laptop because there was ample evidence both violations in the FBI's letter. R. at 15-16, 18.

CONCLUSION

The Fourth Amendment does not disappear at the border. A forensic digital search of a traveler's most private information is a non-routine border search that

requires reasonable suspicion. And for a forensic digital search to have any connection to the rationale for permitting warrantless border searches, officials must reasonably suspect a device contains digital contraband. Petitioner thus asks this Court to reverse the decision of the Tenth Circuit Court of Appeals and grant his motion to suppress the evidence obtained in the unreasonable and unconstitutional search of his private digital data.

Dated: February 22, 2021

Respectfully submitted,

_____

DANIKA KRITTER

Counsel for Petitioner