Vanderbilt Journal of Entertainment & Technology Law

Volume 24
Issue 4 *Summer 2022*

Article 5

2022

Putting Cano on ICE – A Path Forward for Border Searches of Electronic Devices

Davis Price Shugrue

Putting Cano on ICE – A Path Forward for Border Searches of Electronic Devices

ABSTRACT

Across the country, circuit courts disagree over what level of suspicion, if any, is required for border officials to search electronic devices. This leaves law enforcement agencies in the lurch because they must craft nationwide policies that cover jurisdictions with differing rules. The Supreme Court should bring this quandary to an end by holding that no reasonable suspicion or warrant is required for border searches of electronic devices. Many scholars and litigants have called for a reasonable suspicion or warrant requirement in light of Supreme Court decisions like Riley *and* Carpenter *that recognize the privacy concerns raised by searches of electronic devices. However, a reasonable suspicion or warrant requirement fails to account for the overwhelming government interests at the US border, including ensuring national security, controlling who and what enters the country, and combatting transnational crime.*

This Note calls upon the Supreme Court to reject limitations on border searches and hold that no reasonable suspicion or warrant is required for searches of electronic devices at the border. This holding recognizes the government's paramount interests and leaves room for Congress to legislate additional protections as technology evolves.

TABLE OF CONTENTS

On an average day, officials at the border process more than one million travelers entering the United States.[1] For a handful of those travelers, this processing includes a search of their electronic devices.[2] Under the "border search" exception to the Fourth Amendment's warrant requirement, travelers crossing the border are subject to a wide range of searches without any individualized suspicion requirement.[3] In recent years, the border search doctrine has run headlong into

1. This includes individuals crossing the border overland via ports of entry and those entering the United States at the functional equivalent of the border, such as by ship or plane. *On a Typical Day in Fiscal Year 2019, CBP…*, U.S. CUSTOMS & BORDER PROT., https://www.cbp.gov/newsroom/stats/typical-day-fy2019 [perma.cc/U235-2C64] (Jan. 28, 2021). Fiscal Year 2019 is the most recent data from prior to the COVID-19 pandemic. *See id.*

2. In Fiscal Year 2020, Customs and Border Protection searched the electronic devices of less than .1% of the travelers they processed. *CBP Enforcement Statistics Fiscal Year 2021*, U.S. CUSTOMS & BORDER PROT., https://www.cbp.gov/newsroom/stats/cbp-enforcement-statistics [https://perma.cc/TD2Y-AWU5] (last visited Mar. 29, 2022).

3. *E.g.* United States v. Flores-Montano, 541 U.S. 149, 155–56 (2004) (requiring no individualized suspicion to remove and search the gas tank of a passenger vehicle crossing the border); *see also* United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985) ("Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant."); Carroll v. United States, 267 U.S. 132, 154 (1925) ("Travelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in."). The Fourth Amendment guarantees that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. However, the "border search" exception has been "a longstanding, historically recognized exception to the Fourth Amendment's general principle that a warrant be obtained." United States v. Ramsey, 431 U.S. 606, 621 (1977); *see infra* Section I.C.

changing technological realities.[4] The electronic devices many people carry with them when traveling raise privacy questions beyond those raised by searches of non-electronics.[5] In 2011, a mere 35 percent of US residents reported owning a smartphone.[6] Today, however, 97 percent of US residents own a cell phone, with 85 percent owning a smartphone.[7] As cell phones have become more prevalent, the privacy interest implicated by cell phones and other electronic devices has increased.[8] Today, a cell phone, laptop, or even USB storage device carries far more data than a similar device did a decade ago.[9] As people carry more personal information with them on electronic devices, privacy advocates and criminal defendants have raised concerns regarding government officials' abilities to search these devices, both at the border and elsewhere.[10]

In the last decade, privacy concerns surrounding cell phones have reared their head at the border, where every year officials search thousands of cell phones, laptops, and other electronic devices.[11] These searches have various goals, including intercepting child sexual abuse material.[12] Searches of electronic devices can be separated into two

---

4. *See, e.g.*, United States v. Cano, 934 F.3d 1002 (9th Cir. 2019).

5. *See, e.g.*, Riley v. California, 573 U.S. 373, 393 (2014) ("Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.").

6. *Id.*

7. Additionally, 77 percent of US residents own a desktop or laptop computer, and 53 percent own a tablet computer. *Mobile Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), http://www.pewinternet.org/fact-sheet/mobile/ [https://perma.cc/ZAY7-YAAN].

8. *See, e.g.*, *Riley*, 573 U.S. at 393–94 (noting that the increased storage capacity of cell phones leads to increased privacy interests).

9. *See, e.g.*, Sujeong Lim, *Average Storage Capacity in Smartphones to Cross 80GB by End-2019*, COUNTERPOINT (Mar. 16, 2019), https://www.counterpointresearch.com/average-storage-capacity-smartphones-cross-80gb-end-2019/ [https://perma.cc/YSP2-GJF4] (indicating the average storage capacity of cell phones doubled from 2017 to 2019).

10. *See, e.g.*, Masood Farivar, *At US Border, Dramatic Spike in Searches of Phones, Electronic Devices*, VOICE OF AM. (Oct. 28, 2017, 2:21 AM), https://www.voanews.com/a/us-border-spike-in-searches-of-phones-electronic-devices/4090013.html [https://perma.cc/XJN8-QETC] (highlighting that searches of electronic devices at the border have "sparked fresh legal challenges from digital rights advocates and defendants in several criminal cases").

11. *CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics*, U.S. CUSTOMS & BORDER PROT., https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and# [https://perma.cc/Z7RE-FLU9] (Feb. 3, 2021) ("In FY17, CBP conducted 30,200 border searches . . . ."); *CBP Enforcement Statistics Fiscal Year 2021*, *supra* note 2 (revealing that CBP conducted 32,038 searches of electronic devices in FY 2020) [hereinafter CBP FY17 STATISTICS].

12. *See, e.g.*, United States v. Aigbekaen, 943 F.3d 713, 718 (4th Cir. 2019); United States v. Touset, 890 F.3d 1227, 1230 (11th Cir. 2018); CBP FY17 STATISTICS, *supra* note 11 ("CBP border searches of electronic devices have resulted in evidence helpful in combating terrorist activity, [child sexual abuse material], violations of export controls, intellectual property rights violations,

general categories: manual searches and forensic searches. A manual (or "basic") search occurs when an officer searches a device by hand without any assistance from an external device or software.[13] A forensic (or "advanced") search, on the other hand, involves connecting the device to be searched to another separate device with extraction capabilities, which is used to extract data from the searched device.[14] Forensic searches can extract data not normally visible to a user, such as data deleted by the user but still contained on the device.[15]

The two agencies tasked with safeguarding the US border, US Customs and Border Protection (CBP) and US Immigration and Customs Enforcement (ICE), both allow their officers and agents to manually search electronic devices at the border without a warrant.[16] Courts across the United States disagree over whether the border search exception to the Fourth Amendment allows searches of electronic devices at the border without individualized suspicion.[17] The US Court of Appeals for the Ninth Circuit recently used the issue of border searches of electronic devices to significantly limit the border search exception as a whole, limiting the exception to searches for contraband.[18]

---

and visa fraud."). Although commonly referred to as "child pornography," this Note will use the terminology "child sexual abuse material" to more accurately reflect the ongoing damage and victimization that occurs each time these images and videos are shared. *See generally Child Sexual Abuse Material*, NAT'L CTR. FOR MISSING & EXPLOITED CHILD., https://www.missingkids.org/theissues/csam [https://perma.cc/ZFA5-KZW9] (last visited Mar. 29, 2022); *Glossary of Terms*, INT'L CTR. FOR MISSING & EXPLOITED CHILD., https://www.icmec.org/resources/glossary/ [https://perma.cc/JER4-9UGU] (last visited Mar. 29, 2022); *Appropriate Terminology*, INTERPOL, https://www.interpol.int/en/Crimes/Crimes-against-children/Appropriate-terminology [https://perma.cc/WK86-HBMQ] (last visited Mar. 29, 2022).

13. Alasaad v. Mayorkas, 988 F.3d 8, 13 (1st Cir. 2021).

14. *Id.* The terms "forensic" and "advanced" are used interchangeably by courts and law enforcement agencies and will be used interchangeably in this Note.

15. United States v. Kolsuz, 185 F. Supp. 3d 843, 849 & n.8 (E.D. Va. 2016), *aff'd*, 890 F.3d 133 (4th Cir. 2018).

16. U.S. CUSTOMS & BORDER PROT., CBP DIRECTIVE NO. 3340-049A, BORDER SEARCH OF ELECTRONIC DEVICES (2018), https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf [https://perma.cc/CYJ4-82L8] [hereinafter CBP DIRECTIVE]; U.S. IMMIGR. & CUSTOMS ENF'T, ICE DIRECTIVE NO. 7-6.1, BORDER SEARCHES OF ELECTRONIC DEVICES (2009), https://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf [https://perma.cc/HWX6-4TJS] [hereinafter ICE DIRECTIVE].

17. *Compare Alasaad*, 988 F.3d at 18 (holding searches of electronic devices at the border never require individualized suspicion), *with* United States v. Cano, 934 F.3d 1002, 1016 (9th Cir. 2019) (holding some searches of electronic devices at the border require reasonable suspicion that contraband is on the device).

18. *Cano*, 934 F.3d at 1018.

Part I of this Note provides useful background information and a history of the Fourth Amendment's border search exception. In Part II, this Note outlines the current landscape of searches of electronic devices at the border, including the ongoing circuit split, the Supreme Court's recent denial of certiorari to a case that could have resolved this split, and prior scholarship about the topic. Finally, Part III proposes that the Supreme Court resolve the circuit split by holding that the Fourth Amendment does not require reasonable suspicion or a warrant for border searches of electronic devices, thus explicitly rejecting the Ninth Circuit's holdings in *United States v. Cano*.[19]

I. BACKGROUND AND HISTORY OF BORDER SEARCH

A. Agency Rules on Border Searches of Electronic Devices

Both CBP and ICE have agency policies that describe when their officers and agents are allowed to search electronic devices at the border;[20] these policies also cover locations that are the functional equivalent of the border, such as international airports.[21] CBP's policy lays out two types of searches: basic and advanced.[22] An advanced search occurs when an investigator connects the electronic device in question to another device or piece of equipment in order to "review, copy, and/or analyze its contents."[23] A basic (or "manual") search is any search other than an advanced search.[24] ICE's original 2009 policy on border searches of electronic devices did not differentiate between basic and advanced searches, but since May 11, 2018, ICE has distinguished them.[25] Through the 2018 update, ICE's policy now mirrors the requirements of CBP's policy,[26] which requires reasonable suspicion for advanced searches, but no individualized suspicion of any kind for basic searches.[27]

19. *Id.* at 1002, 1018.
20. *See generally* CBP DIRECTIVE, *supra* note 16; ICE DIRECTIVE, *supra* note 16.
21. CBP DIRECTIVE, *supra* note 16, at 2; ICE DIRECTIVE, *supra* note 16, at 1.
22. CBP DIRECTIVE, *supra* note 16, at 4–5.
23. *Id.* at 5.
24. *Id.* at 4.
25. Alasaad v. Mayorkas, 988 F.3d 8, 14 (1st Cir. 2021).
26. *Id.*
27. CBP DIRECTIVE, *supra* note 16, at 4–5.

Each year, thousands of electronic devices are searched at the border.[28] However, these searches are exceedingly rare compared to the number of individuals that annually travel in and out of the United States.[29] In the 2017 fiscal year, CBP processed nearly four hundred million travelers entering the United States.[30] Of those travelers, approximately thirty thousand had an electronic device searched, which amounts to less than one out of every ten thousand inbound travelers.[31] These numbers do not account for searches of outbound passengers, who are also subject to border searches.[32]

B. Recent Supreme Court Rulings Regarding Cell Phones

In recent years, the Supreme Court has decided two prominent cases regarding law enforcement searches of cell phones.[33] Neither dealt with the border search exception specifically.[34] However, both cases restrict law enforcement's ability to search cell phones.[35] Further, both decisions note the unique and extensive privacy interests in the phones.[36] *Carpenter v. United States* and *Riley v. United States* are commonly cited by proponents of a warrant requirement for searches of electronic devices at the border to argue that electronic devices, such as cell phones, pose unique Fourth Amendment questions.[37]

Carpenter is the more recent case of the pair, but is less relevant to border search questions.[38] The Court in *Carpenter* found that the

28. CBP FY17 STATISTICS, *supra* note 11 (reporting that CPB conducted 30,200 border searches in fiscal year 2017); Farivar, *supra* note 10 (estimating CBP searched 30,000 electronic devices in 2017).

29. *Compare supra* note 1 and accompanying text, *with supra* note 28 and accompanying text.

30. CBP FY17 STATISTICS, *supra* note 11.

31. *Id.*

32. *E.g.*, United States v. Kolsuz, 890 F.3d 133, 137–38 (4th Cir. 2018) (involving a border search of an outbound traveler's cell phone).

33. *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018); Riley v. California, 573 U.S. 373 (2014).

34. *See Carpenter*, 138 S. Ct. 2206; *Riley*, 573 U.S. 373.

35. *Carpenter*, 138 S. Ct. at 2223; *Riley*, 573 U.S. at 403.

36. *See Carpenter*, 138 S. Ct. at 2218; *Riley*, 573 U.S. at 393.

37. *See, e.g.*, Rebecca M. Rowland, Note, *Border Searches of Electronic Devices*, 97 WASH. U. L. REV. 545, 552 (2019) ("Together *Riley* and *Carpenter* set forth a strong defense for the protection of digital data from warrantless searches."); Sean O'Grady, Note, *All Watched Over by Machines of Loving Grace: Border Searches of Electronic Devices in the Digital Age*, 87 FORDHAM L. REV. 2255, 2281 (2019) ("[A]ll border searches of electronic devices should be considered nonroutine in light of the emphasis in *Riley* and *Carpenter* on the substantial privacy interests that individuals possess in their digital data stored on electronic devices."); s*ee also Carpenter*, 138 S. Ct. 2206; *Riley*, 573 U.S. 373.

38. *See Carpenter*, 138 S. Ct. 2206.

government needed a warrant to obtain cell-site location information.[39] Location information is generated automatically and without the user's knowledge as his or her cell phone connects to the nearest cell site to communicate with the carrier's wireless network.[40] Although *Carpenter*'s holding on cell-site location information is not directly applicable to border searches, its commentary on the privacy concerns surrounding cell phones may be relevant.[41]

More applicable to border searches is *Riley*, which examines the application of the "search incident to arrest" exception to cell phones.[42] Search incident to arrest is an exception to the Fourth Amendment's warrant requirement which allows police officers to search a person arrested for officer safety reasons and prevent the destruction of evidence.[43] The petitioner in *Riley* was arrested on weapons charges after a traffic stop.[44] Upon the petitioner's arrest, the arresting officer seized his cell phone and began to search it.[45] Eventually, the officer found a photograph on the phone, linking the petitioner to a recent shooting, and the petitioner moved to suppress this evidence when he was charged in relation to the shooting.[46]

The *Riley* Court decided in favor of the petitioner, ruling that the search incident to arrest exception generally does not allow police officers to search an arrestee's cell phone.[47] The Court conducted a balancing test and examined whether the legitimate government interests outweighed the level of intrusion upon the petitioner's privacy.[48] On one hand, the government's interests as they relate to the search incident doctrine are not well served by searching a cell phone.[49] Two primary government interests underlie the search incident doctrine: officer safety and prevention of evidence destruction.[50] In *Riley*, the government's only argument regarding officer safety was that searching a cell phone might alert officers to accomplices or allies who might be on their way to the scene to confront officers.[51] The Court was

39. *Id.* at 2221.

40. *Id.* at 2211–12.

41. *Id.* at 2217–21 (explaining that cell phones allow government officials to conduct intrusive surveillance with less cost and effort than ever before).

42. *Riley*, 573 U.S. at 380, 382–83.

43. *Id.* at 383.

44. *Id.* at 373.

45. *Id.*

46. *Id.*

47. *Id.* at 386.

48. *Id.* at 385–86.

49. *Id.* at 386.

50. *Id.*

51. *Id.* at 387–88.

unconvinced by this argument and pointed to the government's lack of real-world examples to support the conjecture.[52] The Court was equally unconvinced about the danger of evidence destruction if officers are unable to search cell phones after arrests.[53] Here, the Court found that the government's anecdotal examples of evidence destruction via remote data wiping were not enough to show that it was a common concern.[54] Furthermore, there are various measures that officers can take to prevent remote data wipes that do not involve cell phone searches.[55]

The *Riley* Court found that, in contrast with the government's limited and uncertain interests in searching a cell phone after an arrest, people have a significantly greater privacy interest in their cell phones compared to other objects on their person.[56] The sheer scope of data held by cell phones—up to sixty-four gigabytes at the time of *Riley*—differs from the amount of information stored in other mediums, which is constrained by physical limitations.[57] Further, cell phones contain many types of data that a person would not typically carry with them in physical form.[58] Before cell phones, a man might carry a photo of his wife or children in his wallet, whereas today, his phone could carry the equivalent of multiple photo albums. In short, *Riley* acknowledges that cell phone searches involve privacy concerns that are very different from most other searches of items found on one's person.[59]

C. History of Border Search

The Fourth Amendment to the US Constitution states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ."[60] Since James Madison drafted the Fourth Amendment, courts have recognized that searches at the border are fundamentally

52. *Id.*

53. *Id.* at 389–90.

54. *Id.*

55. *Id.* at 390.

56. *Id.* at 393 (stating that comparing the privacy interest in other physical objects to the privacy interest in a cell phone is akin to "saying a ride on horseback is materially indistinguishable from a flight to the moon").

57. *Id.* at 393–34 ("Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy.").

58. *Id.* at 394 (listing photographs, videos, bank statements, and addresses as examples).

59. *See id.*

60. U.S. CONST. amend. IV.

different from searches in the interior of the United States.[61] Just two months before Congress sent the Bill of Rights to the states for ratification, the same Congress adopted the nation's first customs statute.[62] This statute gave customs officers far-reaching power to search and seize goods entering the United States from abroad.[63] The Supreme Court recognized this early customs statute as informative in the interpretation of the Fourth Amendment because it shows that the Congress that proposed the Fourth Amendment viewed searches by customs officers at the border to be reasonable for no reason other than that they occur at the border or the functional equivalent thereof.[64]

The high-water mark for border search arguably came in 1977 in *United States v. Ramsey*.[65] The defendant in *Ramsey* asked the Supreme Court to require probable cause or a warrant for customs officers to search inbound mail from foreign countries.[66] The Court rejected this invitation.[67] The Court's commentary in *Ramsey* on border search as a general matter may be relevant when considering border searches of electronic devices.[68] Justice Rehnquist, writing for the majority, stated that border searches "from before the adoption of the Fourth Amendment, have been considered to be 'reasonable' by the single fact that the person or item in question had entered our country from outside."[69] According to Justice Rehnquist, border searches are per se reasonable under the Fourth Amendment because they occur at the border.[70] Thus, by this logic, almost any search at the border is permissible under the Fourth Amendment.

To see how far the Supreme Court has stretched the border search exception to allow searches of property without reasonable suspicion, one need look no further than *United States v. Flores-Montano*.[71] Officers at the border seized more than eighty pounds of marijuana from the gas tank of the respondent's 1987 Ford Taurus.[72] When the respondent's case went to court in the Southern District of

61. United States v. Ramsey, 431 U.S. 606, 616 (1977).

62. *Id.*

63. *Id.*

64. *See id.* at 617–18; Boyd v. United States, 116 U.S. 616, 623 (1886) ("[I]t is clear that the members of that body did not regard searches and seizures of this kind as 'unreasonable,' and they are not embraced within the prohibition of the amendment.").

65. 431 U.S. 606.

66. *Id.* at 607–09.

67. *Id.* at 608.

68. *See id.* at 619.

69. *Id.*

70. *Id.*

71. *See generally* United States v. Flores-Montano, 541 U.S. 149 (2004).

72. *Id.* at 150.

California, the government did not argue that the officers who searched the respondent's vehicle had a warrant, probable cause, or even reasonable suspicion.[73] Instead, the government argued that the officers were allowed to raise the vehicle up on a mechanical lift, unfasten a series of straps and bolts, and physically remove the gas tank from the vehicle simply because this search occurred at a port of entry.[74]

Both the district court and the Ninth Circuit were unconvinced by the government's argument and held that reasonable suspicion is required before the government can break out its power tools and mechanical lifts to remove a person's gas tank.[75] The Ninth Circuit did so summarily, without issuing a written opinion.[76] In stark contrast, the Supreme Court unanimously reversed.[77] Although the Court in *Flores-Montano* explicitly stated that it was not making any decision regarding the level of suspicion required for "highly intrusive searches of the person," it held that no level of suspicion was required for the type of gas tank search at issue.[78] Notably, the Court declined to form a balancing test to determine what constitutes a "routine" border search.[79]

However, the Supreme Court has come closer to limiting government conduct with respect to invasive searches of the person.[80] In *United States v. Montoya de Hernandez*, the Court examined the case of a traveler entering Los Angeles (LA) on a flight from Bogota, Colombia.[81] The respondent traveled to LA alone and recently made multiple other trips to LA and Miami.[82] Her explanation for the visit did not add up—she was not packed appropriately for LA weather, had no hotel reservations, and did not know how her airline ticket had been bought.[83] Based on her behavior, the inconsistencies of her story, and Bogota's reputation as an origin city for narcotics, the customs officers at LA International Airport suspected the respondent was a "balloon

73. *Id.* at 151.
74. *Id.* at 151–52.
75. *Id.* at 151.
76. *Id.*
77. *Id.* at 150–51.
78. *Id.* at 152, 155.
79. *Id.* at 152.
80. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 533 (1985).
81. *Id.* at 532.
82. *Id.* at 533.
83. *Id.* at 533–34.

swallower"—someone who smuggles narcotics in their alimentary canal by swallowing and then passing them after clearing customs.[84]

At this point, officers gave the respondent three choices: leave on the next flight bound for Colombia, consent to an X-ray of her alimentary canal, or remain in detention until she produced a bowel movement in which officers could search for narcotics.[85] She initially chose the x-ray, but changed her mind and asked to return to Colombia.[86] Officers could not get the respondent on a direct flight to Colombia for many hours,[87] and after holding her for sixteen hours, they obtained a court order for an x-ray.[88] Throughout her detention, the respondent became increasingly uncomfortable as she engaged in what the Ninth Circuit dubbed, "heroic efforts to resist the usual calls of nature."[89] Following an examination, a physician recovered eighty-eight balloons containing more than a pound of cocaine from the respondent's alimentary canal.[90] The Court held that the respondent's detention, although beyond the scope of a routine border search, was permissible because customs agents were in possession of facts that "clearly supported a reasonable suspicion that respondent was an alimentary canal smuggler."[91] However, the Court's rule in the case is narrow, applying only to situations where agents reasonably suspect a traveler is an alimentary canal smuggler.[92]

84. *Id.*

85. *Id.* at 534–35.

86. *Id.* at 535.

87. The officers attempted to place Montoya de Hernandez on a flight to Bogota connecting through Mexico City, but the airline refused to allow her to board because she did not have the proper visa to enter Mexico. *Id.*

88. *Id.*

89. United States v. Montoya de Hernandez, 731 F.2d 1369, 1371 (1984).

90. *Montoya de Hernandez*, 473 U.S. at 536–37.

91. *Id.* at 542.

92. *Id.* at 541.

II. THE CURRENT LANDSCAPE OF BORDER SEARCHES OF ELECTRONIC DEVICES

A. The Legal Landscape—A Circuit Split

In the wake of *Flores-Montano* and *Montoya de Hernandez*,[93] lower courts have disagreed over what level of suspicion—if any—is required to search electronic devices at the border.[94]

1. The Ninth Circuit's Restrictive Approach

On one end of the spectrum sits the Ninth Circuit. In 2019, the Ninth Circuit dramatically curtailed border searches of electronic devices in *Cano*.[95] The Ninth Circuit's *Cano* decision represents a major restriction on border searches of electronic devices.[96] Even though the Ninth Circuit concluded in 2013 that manually searching cell phones does not require reasonable suspicion, *Cano* imposes a reasonable suspicion requirement on forensic searches.[97] In addition to this reasonable suspicion requirement, *Cano* holds that the Fourth Amendment's border search exception is limited to searches for contraband.[98]

In *Cano*, the Ninth Circuit dealt with a search of the respondent's cell phone.[99] The respondent attempted to enter the United States at the San Ysidro port of entry, where his vehicle was sent for a secondary inspection.[100] After a narcotics-detecting canine signaled that it detected the odor of narcotics near the vehicle's spare tire, CBP officers searched the tire and discovered more than thirty pounds of cocaine.[101] Following this search, ICE Homeland Security Investigations agents seized the respondent's phone and searched it, first manually and then forensically.[102] The agents did not obtain a warrant for these searches.[103] According to the agents, the purpose of

93. *See generally id.*; United States v. Flores-Montano, 541 U.S. 149 (2004).

94. *Compare* United States v. Cotterman, 709 F.3d 952, 962 (9th Cir. 2013) (holding forensic searches require reasonable suspicion), *with* United States v. Touset, 890 F.3d 1227, 1231 (11th Cir. 2018) (holding forensic searches do not require reasonable suspicion).

95. *See* United States v. Cano, 934 F.3d 1002 (9th Cir. 2019).

96. *See id.* at 1007.

97. *Id.*

98. *Id.* at 1020.

99. *Id.* at 1007.

100. *Id.* at 1008.

101. *Id.*

102. *Id.* at 1008–09.

103. *Id.*

their search was not to locate digital contraband, such as child sexual abuse material, but to find either "investigative leads" regarding the respondent's case or "evidence of other things coming across the border."[104] The Ninth Circuit found that both the manual and forensic search violated the Fourth Amendment because they exceeded the scope of the border search exception to the Fourth Amendment's warrant requirement.[105] Thus, *Cano* strictly limits border search to searches for contraband; searches for evidence of contraband or evidence of ongoing border-related crime are not included in the Ninth Circuit's purview.[106]

2. The First and Eleventh Circuits' Permissive Approaches

In stark contrast to *Cano* are a pair of cases from the First and Eleventh Circuits.[107] The first, *United States v. Touset*, is an Eleventh Circuit decision which holds that no suspicion is required for searches of electronic devices at the border.[108] The second, *Alasaad v. Mayorkas*, is a First Circuit case that rejects both of *Cano*'s holdings.[109]

On December 21, 2014, a CBP officer at Hartsfield-Jackson Atlanta International Airport inspected the defendant's luggage after he entered the United States.[110] The officer was alerted to the defendant by a "look-out" from Homeland Security's Cyber Crime Center, which indicated officers should search the defendant's electronic devices for child sexual abuse material.[111] CBP conducted forensic searches of two laptops and two external hard drives confiscated from the defendant and located child sexual abuse material on all four devices.[112] ICE then used the information from those searches to obtain a search warrant for the defendant's residence, where agents located thousands of pieces of child sexual abuse material.[113] The defendant moved to suppress the evidence on the grounds that the original forensic search at the border was a violation of his Fourth Amendment rights, and the resulting

104. *Id.* at 1008.

105. *Id.* at 1022.

106. *See id.* at 1019.

107. *Compare Cano*, 934 F.3d 1002, *with* United States v. Touset, 890 F.3d 1227 (11th Cir. 2018), *and* Alasaad v. Mayorkas, 988 F.3d 8 (1st Cir. 2021).

108. *Touset*, 890 F.3d at 1231.

109. *Alasaad*, 988 F.3d at 20–21 ("We cannot agree with its narrow view of the border search exception because *Cano* fails to appreciate the full range of justifications for the border search exception beyond the prevention of contraband itself entering the country.").

110. *Touset*, 890 F.3d at 1230.

111. *Id.*

112. *Id.*

113. *Id.*

evidence was the fruit of that unconstitutional search.[114] The lower court denied the defendant's motion; he agreed to a plea deal in exchange for a ten-year prison sentence, but reserved his right to appeal the denial of his motion to suppress.[115]

The lower court in *Touset* denied the defendant's motion to suppress, holding that the forensic search required reasonable suspicion and the government met that requirement.[116] The Eleventh Circuit affirmed, holding that the border search exception allows manual and forensic searches of electronic devices without suspicion.[117] The court stated that searches of property at the border are "reasonable without suspicion 'simply by virtue of the fact that they occur at the border.'"[118] The court further noted that neither the Eleventh Circuit nor the Supreme Court had ever required reasonable suspicion for searches of property at the border.[119] According to the *Touset* court, only searches of a person ever require reasonable suspicion; no border searches of property, regardless of privacy interests, require reasonable suspicion.[120]

In *Alasaad*, the First Circuit addressed a challenge brought by a group of US citizens and a lawful permanent resident, all of whom alleged that ICE or CBP searched their electronic devices on one or more occasions.[121] The US District Court for the District of Massachusetts held that both manual and forensic searches require reasonable suspicion, and, as in *Cano*,[122] the border search exception is limited to searches for contraband.[123] The plaintiffs argued that the First Circuit should go even further than the lower court and hold that all searches of electronic devices require a warrant.[124] Instead, the First

114. *Id.* at 1229–31.

115. *Id.* at 1231.

116. *Id.*

117. *Id.* at 1229, 1231–38.

118. *Id.* at 1232 (quoting Denson v. United States, 574 F.3d 1318, 1339 (11th Cir. 2009)).

119. *Touset*, 890 F.3d at 1233 ("The Supreme Court has never required reasonable suspicion for a search of property at the border, however non-routine and intrusive, and neither have we.").

120. *See id.*; *see also* United States v. Alfaro-Moncada, 607 F.3d 720, 728–31 (11th Cir. 2010) (holding reasonable suspicion is not required to search crew cabins on a ship, even though "[a] cabin is a crew member's home" and homes receive the highest level of Fourth Amendment protection).

121. Alasaad v. Mayorkas, 988 F.3d 8, 14 (1st Cir. 2021).

122. United States v. Cano, 934 F.3d 1002, 1007 (9th Cir. 2019).

123. *Alasaad*, 988 F.3d at 15.

124. *Id.* at 16.

Circuit held that both manual and forensic searches do not require reasonable suspicion.[125]

Alasaad also directly addressed and rejected *Cano*'s contraband limitation on border searches.[126] The First Circuit defined the purpose of border searches as controlling "who and what may enter the country."[127] Based on this wider purpose, the First Circuit held that the scope of border searches includes contraband and extends to evidence of contraband or border-related crime.[128] Also noteworthy, the court addressed and rejected the invitation to extend the Supreme Court's *Riley* holding to the border search context.[129]

B. The Scholarly Landscape—In Favor of a Reasonable Suspicion or Warrant Requirement

Most legal scholarship favors requiring either reasonable suspicion or a warrant for border searches of electronic devices.[130] Arguments in favor of such heightened requirements tend to contain two general points: (1) electronic devices carry heightened privacy interests, and (2) searches of electronic devices do not support the purposes of the border search exception.[131]

Proponents of a reasonable suspicion or warrant requirement argue that cell phones and other electronic devices carry heightened privacy interests compared to other property.[132] Computers and other electronic devices have storage capacities that exceed all other mediums

---

125. *Id.* at 19.

126. *Id.* at 20–21.

127. *Id.* at 20 (quoting United States v. Ramsey, 431 U.S. 606, 620 (1977)).

128. *Alasaad*, 988 F.3d at 21.

129. *Id.* at 17 ("Contrary to plaintiffs' assertions, *Riley* does not command a warrant requirement for border searches of electronic devices nor does the logic behind *Riley* compel us to impose one.").

130. *See, e.g.*, O'Grady, *supra* note 37 (advocating a reasonable suspicion requirement); Ashley N. Gomez, Comment, *Over the Border, Under What Law: The Circuit Split over Searches of Electronic Devices on the Border*, 52 ARIZ. ST. L.J. 279 (2020) (advocating a reasonable suspicion requirement); Gina R. Bohannon, Comment, *Cell Phones and the Border Search Exception: Circuits Split over the Line Between Sovereignty and Privacy*, 78 MD. L. REV. 563 (2019) (advocating a warrant requirement); Rowland, *supra* note 37 (advocating a warrant requirement). *But see* Michael Creta, Comment, *A Step in the Wrong Direction: The Ninth Circuit Requires Reasonable Suspicion for Forensic Examinations of Electronic Storage Devices During Border Searches in* United States v. Cotterman, 55 B.C. L. REV. ELEC. SUPPLEMENT 31 (2014) (advocating against a reasonable suspicion requirement).

131. *See, e.g.*, Bohannon, *supra* note 130, at 588–91, 594–97.

132. *Supra* notes 128–31 and accompanying text; *infra* notes 133–35 and accompanying text.

of information.[133] The sheer quantity of information on electronic devices surpasses the amount of information that border officers could find before the advent of these devices.[134] Yet the quantity of information is not the only concern; often, the personal nature of the information stored on electronic devices also raises privacy concerns.[135] Electronic devices carry sensitive information, such as bank and medical records.[136] These devices also often carry communications like text messages and emails.[137] Finally, the role that cell phones and other electronic devices play in everyday life also raises privacy concerns. The border search exception is limited to searches at the border or its functional equivalents, such as international airports.[138] Thus, individuals can ordinarily avoid subjecting property to a border search by not carrying it across the border.[139] However, with cell phones and other electronic devices, this is often easier said than done; most people

133. *See* United States v. Cotterman, 709 F.3d 952, 964 (9th Cir. 2013) (explaining the average laptop hard drive at the time could store "the equivalent of five floors of a typical academic library"); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 542 (2005) (explaining an 80-gigabyte hard drive stores the equivalent of 40 million pages of information, approximately one floor of an academic library).

134. United States v. Kolsuz, 890 F.3d 133, 145 (4th Cir. 2018) ("The sheer quantity of data stored on smartphones and other digital devices dwarfs the amount of personal information that can be carried over a border—and thus subjected to a routine border search—in luggage or a car."); *Cotterman*, 709 F.3d at 964 ("Even a car full of packed suitcases with sensitive documents cannot hold a candle to the sheer, and ever-increasing, capacity of digital storage."); Bohannon, *supra* note 130, at 589.

135. *See Kolsuz*, 890 F.3d at 145 (noting the "uniquely sensitive nature" of the information electronic devices contain); *Cotterman*, 709 F.3d at 964 (highlighting that electronic devices "contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails"); Kathryn Neubauer, Note, *Unlock Your Phone and Let Me Read All Your Personal Content, Please: The First and Fifth Amendments and Border Searches of Electronic Devices*, 92 S. CAL. L. REV. 1273, 1276 (2019) (discussing how electronic devices store "extremely personal data"); O'Grady, *supra* note 37, at 2269 (acknowledging that searches of electronic devices reveal "intimate data" and are "as intrusive as strip searches or body-cavity searches").

136. Riley v. California, 573 U.S. 373, 400 (2014) (suggesting that a cell phone may contain "every bank statement from the last five years"); Bohannon, *supra* note 130, at 590; Rowland, *supra* note 37, at 550 (noting cell phones can contain prescription and banking information).

137. *Kolsuz*, 890 F.3d at 145 (stating electronic devices carry private emails); *Cotterman*, 709 F.3d at 964 (noting electronic devices carry private emails); Neubauer, *supra* note 135, at 1283; Bohannon, *supra* note 130, at 590 (mentioning electronic devices carry spousal communications); Sid Nadkarni, Comment, *"Let's Have a Look, Shall We?" A Model for Evaluating Suspicionless Border Searches of Portable Electronic Devices*, 61 UCLA L. REV. 146, 149 (2013) (describing how an individual whose laptop was searched by CBP found that agents viewed "transcripts of chats with his girlfriend" and "copies of emails").

138. *Supra* note 21 and accompanying text.

139. *See supra* note 21 and accompanying text.

carry cell phones and electronic devices with them constantly as a part of their everyday lives.[140]

The second main argument in favor of a reasonable suspicion or warrant requirement is that cell phones and other electronic devices do not support the purposes of the border search exception.[141] According to this argument, border searches of cell phones and other electronic devices are not actually fulfilling the border search exception's purpose of controlling who and what enters the country.[142] Instead, proponents of heightened suspicion requirements argue that these searches are used to either harass innocent travelers, or, more commonly, as "fishing expeditions" to enforce laws unrelated to the border.[143] As such, heightened suspicion proponents advocate limiting the border search exception's applicability to electronic devices.[144]

C. Supreme Court Silence

The Supreme Court has yet to rule on what level of individualized suspicion, if any, is required to search electronic devices at the border. The Court rejected three petitions for a grant of certiorari in 2021 that could have resolved the ongoing split amongst lower courts.[145] Two of those were for cases discussed extensively in this Note: *Alasaad* and *Cano*.[146]

---

140. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) (asserting that individuals "compulsively carry cell phones with them"); *Riley*, 573 U.S. at 395 ("Now it is the person who is not carrying a cell phone . . . who is the exception."); Neubauer, *supra* note 135, at 1315.

141. *See, e.g.*, Bohannon, *supra* note 130, at 596–97; Nadkarni, *supra* note 137, at 193–94.

142. *See, e.g.*, Bohannon, *supra* note 130, at 598–99; Nadkarni, *supra* note 137, at 173–74.

143. *See, e.g.*, Bohannon, *supra* note 130, at 598–99; Nadkarni, *supra* note 137, at 173–74; Alasaad v. Nielsen, No. 17-CV-11730-DJC, 2018 WL 2170323, at *5 (D. Mass. May 9, 2018) (alleging CBP supervisor told plaintiffs he ordered a search of their cell phones because he "felt like" doing so).

144. *See supra* note 130 and accompanying text.

145. Aigbekaen v. United States, 141 S. Ct. 2871 (2021) (mem.); United States v. Cano, 141 S. Ct. 2877 (2021) (mem.); Merchant v. Mayorkas, 141 S. Ct. 2858 (2021) (mem.).

146. *See* United States v. Cano, 934 F.3d 1002 (9th Cir. 2019), *cert. denied*, 141 S. Ct. 2877; Alasaad v. Mayorkas, 988 F.3d 8 (1st Cir. 2021), *cert. denied*, 141 S. Ct. 2858; *see also supra* Part II.

III. SOLUTION: NO REASONABLE SUSPICION, NO RESTRICTION TO CONTRABAND ONLY, AND ROOM TO LEGISLATE ADDITIONAL PROTECTIONS

The Supreme Court should resolve the current circuit split by ruling that the border search exception to the Fourth Amendment's warrant requirement allows searches of electronic devices without reasonable suspicion. The Supreme Court should also reject the Ninth Circuit's limitation of border searches in *Cano* by ruling that the border search exception is not limited to searches for contraband.[147] These holdings would vindicate the longstanding history of border searches, properly recognize the government's overwhelming interests at the border, and create a constitutional floor from which Congress can add additional protections if and when they become necessary. A Supreme Court holding that border searches of electronic devices do not require reasonable suspicion is unlikely to lead to a dramatic alteration in the number or nature of electronic devices searched by border officials.[148]

The Supreme Court should address the circuit split to create nationwide uniformity. The current split amongst circuit courts is untenable for the executive and legislative branches. CBP and ICE, both executive branch agencies, operate nationwide and are tasked with securing the US border, which includes functional equivalents like international airports.[149] These agencies' policies govern their actions across the country.[150] More restrictive circuits thus effectively impose nationwide limits on CBP and ICE unless the agencies are willing to craft different policies in different circuits. Common sense dictates that the federal government should have the same ability to search electronic devices of inbound international passengers at the airport in Los Angeles as it does in Miami, but the Ninth and Eleventh Circuits have dramatically different standards for warrantless searches of electronic devices at the border.[151] By weighing in on the issue, the Supreme Court can set a clear baseline for electronic device searches at the border and allow the executive branch to freely craft its electronic

147. *See Cano*, 934 F.3d at 1007.

148. *See infra* Section III.D.

149. CBP DIRECTIVE, *supra* note 16, at 2; ICE DIRECTIVE, *supra* note 16, at 1.

150. *See* CBP DIRECTIVE, *supra* note 16 (containing no geographic differentiation for search requirements); ICE DIRECTIVE, *supra* note 16 (containing no geographic differentiation for search requirements).

151. *Compare Cano*, 934 F.3d at 1016–17 (holding forensic searches of an electronic device require reasonable suspicion contraband is contained on the device), *with* United States v. Touset, 890 F.3d 1227, 1231 (11th Cir. 2018) ("[T]he Fourth Amendment does not require any suspicion for forensic searches of electronic devices at the border.").

device search policies without limiting the agencies by requiring that they operate under different rules in different circuits.

A. The Supreme Court Should Hold That No Reasonable Suspicion is Required for Border Searches of Electronic Devices

The Supreme Court should not require reasonable suspicion for any electronic device search—manual or forensic—at the border because the government's interests outweigh privacy interests. Furthermore, Congress is better suited to determine the balance between security and privacy. Reasonable suspicion is the highest requirement for a search at the border; searches at the border "never require a warrant or probable cause."[152] The Supreme Court has only ever required reasonable suspicion for invasive searches of the person, never for property.[153] The distinction between persons and property makes border searches more easily administrable by setting a clear and easy-to-apply rule. Indeed, the Supreme Court in *Flores-Montano* explicitly declined to create "[c]omplex balancing tests" for border searches.[154]

The balance of interests at the border does not justify a reasonable suspicion requirement; as stated previously, the Fourth Amendment's balancing test favors the government more at the border than anywhere else.[155] The government is uniquely interested in protecting national security through border searches.[156] Conversely, travelers have a reduced expectation of privacy when they cross international borders.[157] Moreover, the Supreme Court has historically given border officials wide latitude to search persons and effects entering and leaving the United States.[158] Electronic devices invoke

---

152. United States v. Vergara, 884 F.3d 1309, 1311 (11th Cir. 2018); *see* United States v. Ramsey, 431 U.S. 606, 619 (1977) ("There has never been any . . . requirement that the reasonableness of a border search depended on the existence of probable cause."); *Touset*, 890 F.3d at 1232–33.

153. *Touset*, 890 F.3d at 1233 ("The Supreme Court has never required reasonable suspicion for a search of property at the border, however non-routine and intrusive . . . .").

154. United States v. Flores-Montano, 541 U.S. 149, 152 (2004).

155. *See supra* notes 61–64 and accompanying text; United States v. Montoya de Hernandez, 473 U.S. 531, 539–40 (1985) ("[T]he Fourth Amendment balance between the interests of the Government and the privacy right of the individual is . . . struck much more favorably to the Government at the border.").

156. *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.").

157. *Montoya de Hernandez*, 473 U.S. at 539 ("[T]he expectation of privacy [is] less at the border than in the interior . . . .").

158. *See, e.g.*, *Flores-Montano*, 541 U.S. at 155 (upholding "suspicionless inspections" of vehicle gas tanks at the border); *Montoya de Hernandez*, 473 U.S. at 544 (upholding hours-long

privacy concerns, but these concerns are overcome by the paramount government interests at the border and fail to justify a reasonable suspicion requirement.[159]

The Supreme Court has weighed privacy interests against the government's national security interests at the border before, and it has consistently come down on the government's side. In *Montoya de Hernandez*, the Court noted that in cases of suspected alimentary canal smuggling, the government will "rarely possess probable cause to arrest or search," but found the government's interest in stopping cross-border narcotics smuggling compelling enough to allow detention of suspected smugglers with only reasonable suspicion.[160] Likewise, in *United States v. Villamonte-Marquez*, the Court held that customs officers are permitted by statute and the Fourth Amendment to stop and search any "vessel that is located in waters providing ready access to the open sea" without any suspicion of wrongdoing.[161] This is true even though boats often serve as a dwelling for their owners, meaning boat searches carry greater privacy concerns than searches of other vehicles.[162] The status quo as it relates to border searches strongly favors the government.[163] The government is not asking courts to strip Fourth Amendment protections from travelers; rather, privacy advocates are asking courts to extend Fourth Amendment protection to areas it has never gone before.[164]

In the age of international terrorism, the government's national security interests are stronger than ever.[165] The ease of electronic

---

detention of "suspected alimentary canal smuggler at the border"); United States v. Ramsey, 431 U.S. 606, 623–25 (1977) (upholding warrantless searches of international mail).

159. Riley v. California, 573 U.S. 373, 393 (2014) (stating that comparing the privacy interest in other physical objects to the privacy interest in a cell phone is akin to "saying a ride on horseback is materially indistinguishable from a flight to the moon"); *Flores-Montano*, 541 U.S. at 152 ("[T]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border.").

160. *Montoya de Hernandez*, 473 U.S. at 541–42.

161. United States v. Villamonte-Marquez, 462 U.S. 579, 581, 593 (1983).

162. *See id.* at 605–606 (Brennan, J., dissenting); *see also* United States v. Alfaro-Moncada, 607 F.3d 720, 728–31 (11th Cir. 2010) (holding reasonable suspicion is not required to search crew cabins on a ship, even though "[a] cabin is a crew member's home" and homes receive the highest level of Fourth Amendment protection).

163. *See, e.g.*, United States v. Touset, 890 F.3d 1227, 1233 (11th Cir. 2018). The Supreme Court has never required reasonable suspicion for searches of property, including electronic devices, at the border. *See id.*

164. *See id.*

165. *See* United States v. Kolsuz, 890 F.3d 133, 152 (4th Cir. 2018) (Wilkinson, J., concurring) ("Our new world has brought inconvenience and intrusions on an indiscriminate basis, which none of us welcome, but which most of us undergo in the interest of assuring a larger common good.").

communication has made international criminal and terrorist activities easier to plan today than ever before.[166] The ability of officers and agents at the border to search electronic devices could be decisive in whether a plot succeeds or fails.[167] Despite the new threats posed by electronic devices, privacy advocates seek to change the Fourth Amendment's application at the border, shifting the relative balance between security and privacy away from security.[168]

As for those advocating for a warrant requirement, the response is simple:[169] warrants have never been required for even the most intrusive searches at the border.[170] If a warrant is not required for "highly intrusive searches of the person,"[171] it should not be required for any searches of property, no matter how invasive. Even in the most extreme border search cases like *Montoya de Hernandez*, where the respondent was detained for sixteen hours and not allowed to use the bathroom unmonitored, the Supreme Court required only reasonable suspicion.[172]

Regardless of the proper balance between security and privacy, Congress is better equipped to fashion rules regarding advanced technologies, and the Supreme Court should allow Congress to do so.[173] Even if the Supreme Court decides that the Fourth Amendment does not require any individualized suspicion for searches of electronic devices at the border, the Constitution merely sets the floor.[174] Congress can legislate to provide additional protections and restrictions, and it

166. *See id.*

167. *See id.*

168. It is advocates, not the government, who seek to change the status quo. *See id.* ("To give criminal enterprises the advantage of technological advancements and at the same time impair access of law enforcement to those same developments risks recalibrating the Fourth Amendment balance in a manner that does not comport with reasonableness."); *supra* note 167 and accompanying text.

169. *See, e.g.*, Rowland, *supra* note 37 ("Together *Riley* and *Carpenter* set forth a strong defense for the protection of digital data from warrantless searches.").

170. United States v. Ramsey, 431 U.S. 606, 619 (1977) ("There has never been any . . . requirement that the reasonableness of a border search depended on the existence of probable cause.").

171. United States v. Flores-Montano, 541 U.S. 149, 152 (2004).

172. United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985).

173. Riley v. California, 573 U.S. 373, 408 (2014) (Alito, J., concurring) ("Legislatures . . . are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future."); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 806 (2004).

174. United States v. Jones, 565 U.S. 400, 427–28 (2012) (Alito, J., concurring).

has done so repeatedly in the wake of Supreme Court decisions on the Fourth Amendment's application to new technologies.[175]

New technologies often shift paradigms and challenge the underlying assumptions of old judicial decisions regarding privacy.[176] This causes judicially-made rules regarding technology to become rapidly outdated.[177] One example of this is the Supreme Court's decision in *Katz v. United States*, holding that the government cannot record conversations in a telephone booth without a warrant.[178] When *Katz* was decided in the late 1960s, before the age of cell phones, public telephones were a vital means of communication in the United States.[179] Today, nearly everyone in the United States owns a cell phone, making public phones obsolete.[180]

Congress is best positioned to regulate changing technology because, unlike the courts, Congress can regulate prospectively.[181] Courts are limited to fashioning rules based on a specific set of facts before them.[182] In order for a case to make it to the Supreme Court, it has to pass through a trial court and appellate court, which is challenging in the criminal procedure context because the vast majority of criminal cases end in plea agreements.[183] Moreover, the Supreme Court only hears a few dozen cases per year and often waits until there are multiple circuit court decisions before it takes up an issue.[184] This Note is evidence of the Court's limited capacity; despite published decisions by multiple circuit courts that disagree with each other, the Supreme Court has thus far declined to rule on the level of suspicion required for border searches of electronic devices.[185]

---

175. *See id.*; Omnibus Crime Control and Safe Streets Act of 1968, tit. III, Pub. L. No. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510–2520 (1986)) (imposing additional requirements for electronic surveillance above and beyond those required by the Fourth Amendment); Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848, 1849–50 (codified as amended at 18 U.S.C. § 2511) (extending Title III requirements to emails, text messages, and cell phone conversations); *see also* CHRISTOPHER SLOBOGIN, ADVANCED INTRODUCTION TO U.S. CRIMINAL PROCEDURE 51–53 (2020) (describing the passage of Title III and the ECPA).

176. *See* Kerr, *supra* note 173, at 859–60.

177. *Id.* at 859.

178. *See generally* Katz v. United States, 389 U.S. 347 (1967).

179. Kerr, *supra* note 173, at 866–67.

180. Ninety-seven percent of US residents own a cell phone. *Mobile Fact Sheet*, *supra* note 7.

181. *See* Kerr, *supra* note 173, at 868.

182. *See id.*

183. *Id.*

184. *Id.* at 868–69.

185. *Supra* notes 145–46 and accompanying text.

Unlike the courts, Congress is able to prospectively craft rules to govern a technology before it even hits the market.[186] Congress also has access to a wider range of information than the courts through sources like Congressional hearings.[187] Additionally, multiple Supreme Court Justices have acknowledged the particular difficulties posed by questions of technology and privacy, as well as Congress's comparative advantages in balancing the opposing interests at play.[188] So too, have lower court judges; Judge J. Harvey Wilkinson III of the Fourth Circuit addressed this issue directly in his concurrence in *United States v. Kolsuz*, writing "the standard of reasonableness in the particular context of a border search should be principally a legislative question, not a judicial one."[189] In light of the legislature's advantages, the best thing that the Supreme Court can do is exercise the humility suggested by Justice Breyer, maintain the status quo, and leave the balancing to Congress.[190]

B. The Supreme Court Should Reject Cano*'s Limits on Border Search*

The Supreme Court should reject the Ninth Circuit's limitations on border searches for two reasons.[191] First, contrary to the Ninth Circuit's assertions, it is not clear that border searches must be limited to those that further the purposes of the border search exception.[192] Second, even if this were true, searches for reasons other than locating contraband still further the purposes of the border search exception—controlling who and what enters the country.[193]

---

186. Kerr, *supra* note 173, at 868.

187. *See id.* at 875.

188. Riley v. California, 573 U.S. 373, 408 (2014) (Alito, J., concurring) ("Legislatures . . . are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future."); Stephen Breyer, *Our Democratic Constitution*, 77 N.Y.U. L. REV. 245, 261 (2002) (describing the problem of electronic privacy as "unusually complex" and stating "it suggests a need for judicial caution and humility when certain privacy matters, such as the balance between free speech and privacy, are at issue").

189. United States v. Kolsuz, 890 F.3d 133, 148 (4th Cir. 2018) (Wilkinson, J., concurring).

190. *See* Breyer, *supra* note 188.

191. United States v. Cano, 934 F.3d 1002, 1016–17 (9th Cir. 2019) (holding forensic searches of an electronic device require reasonable suspicion contraband is contained on the device).

192. Alasaad v. Mayorkas, 988 F.3d 8, 19 (1st Cir. 2021) (explaining the Supreme Court's rule in *Riley* limiting warrantless searches to those that advance the purposes of an exception does not, on its face, extend to the border search context).

193. *Id.* ("[A] search for evidence of either contraband or a cross-border crime furthers the purposes of the border search exception . . . ."); *see* United States v. Gurr, 471 F.3d 144 (D.C. Cir.

There is no doubt that searches for contraband implicate the border search exception's purposes.[194] Cell phones and other electronic devices can transport digital contraband across the border.[195] The most serious type of digital contraband, seen in many of the cases referenced in this Note, is child sexual abuse material.[196] However, it is not the only type of digital contraband. For example, the United States restricts the export of certain software and technical data, especially software or data with potential military uses.[197] Another example of digital contraband is pirated software.[198] Border searches of electronic devices help the government control the import and export of digital contraband, fulfilling one of the purposes of the border search exception.[199]

Cell phones and other electronic devices may contain evidence related to contraband smuggling or other cross-border crimes.[200] This evidence is "vital to" controlling who and what enters the country.[201] An opinion authored by then-Judge Anthony Kennedy provides a useful example.[202] In *United States v. Schoor*, the defendant was convicted for his role in a scheme that smuggled narcotics hidden inside radios from Thailand to the United States.[203] Tipped off by Drug Enforcement Agency (DEA) agents, customs officers searched the defendant when he entered the country.[204] The DEA agent asked the officers to search for narcotics and any documents related to air travel or radio shipments.[205]

2006) ("The distinction that [the defendant] would draw between contraband and documentary evidence of a crime is without legal basis.").

194. *See, e.g.*, *Cano*, 934 F.3d at 1013–14 ("We agree . . . the purpose of the border search [exception] is to interdict contraband, but we disagree . . . that cell phones cannot contain contraband.").

195. *See, e.g.*, United States v. Aigbekaen, 943 F.3d 713, 718 (4th Cir. 2019); United States v. Touset, 890 F.3d 1227, 1230 (11th Cir. 2018).

196. *See, e.g.*, *Aigbekaen*, 943 F.3d at 718; *Touset*, 890 F.3d at 1230.

197. *U.S. Export Controls*, INT'L TRADE ADMIN., https://www.trade.gov/us-export-controls [https://perma.cc/Q54J-CUSG] (last visited Apr. 1, 2022); *see also* United States v. Kolsuz, 890 F.3d 133, 152 (4th Cir. 2018) (Wilkinson, J., concurring) ("[T]here is the danger of highly classified technical information being smuggled out of this country only to go into the hands of foreign nations who do not wish us well and who seek to build their armaments to an ever more perilous state.").

198. Nadkarni, *supra* note 137, at 175.

199. *See, e.g.*, *Aigbekaen*, 943 F.3d at 718; *Touset*, 890 F.3d at 1230.

200. *See, e.g.*, Alasaad v. Mayorkas, 988 F.3d 8, 21 (1st Cir. 2021) ("[B]order searches of electronic devices may be used to search for contraband, evidence of contraband, or for evidence of activity in violation of the laws enforced or administered by CBP or ICE.").

201. *Id.* at 20.

202. *See generally* United States v. Schoor, 597 F.2d 1303 (9th Cir. 1979).

203. *Id.* at 1305.

204. *Id.*

205. *Id.*

The officers did not locate narcotics, but they did find documents related to prior radio shipments from Thailand and airline tickets to and from Thailand.[206] The three-judge panel unanimously found the search and seizure of the documents valid, holding that customs officers are entitled to seize "instrumentalities or evidence of crimes."[207] Even though the officers found no actual contraband, their search returned valuable information for disrupting the cross-border shipment of narcotics, thus fulfilling the border search exception's purpose of controlling what enters the country.[208]

Taken on its face, restricting border searches to looking for contraband only leads to absurd results. Consider officers searching a ship. One item the officers will surely want to examine is the manifest.[209] The officers know that they will probably not discover contraband in the manifest's paper and ink. Yet, examining the manifest is useful in the officers' efforts to control who and what enters the country. It may provide details on the origin, destination, and purported contents of the cargo shipment, all valuable information for officers trying to differentiate legitimate cargo from contraband.[210] However, following *Cano*, the manifest would be off-limits unless officers could show that they reasonably suspected it contained contraband.[211] Such a limitation actively hinders the objectives of the border search exception.

Finally, cell phones and other electronic devices may contain evidence related to a person's admissibility into the United States. The Immigration and Nationality Act makes various classes of persons ineligible for admission.[212] Reasons for inadmissibility include past criminal activity, national security concerns, and health concerns.[213] When searching electronic devices, officers often discover information that results in the denial of US entry.[214] Although this information is

206. *Id.*

207. *Id.* at 1306.

208. *Id.*

209. A manifest lists all items aboard a vessel, including ship's stores, crew members' personal effects, and cargo. 19 C.F.R. § 4.7a (2021).

210. *See id.*

211. United States v. Cano, 934 F.3d 1002, 1016 (9th Cir. 2019) (holding some searches of electronic devices at the border require reasonable suspicion contraband is on the device).

212. 8 U.S.C. § 1182.

213. *Id.*

214. *E.g.*, U.S. DEP'T OF HOMELAND SEC., OIG-19-10, CBP'S SEARCHES OF ELECTRONIC DEVICES AT PORTS OF ENTRY 2 (2018), https://www.oig.dhs.gov/sites/default/files/assets/2018-12/OIG-19-10-Nov18.pdf [https://perma.cc/SSD9-4VDK] (discussing how a CBP officer denied a traveler entry after finding terrorist-related materials on the traveler's phone).

not itself illegal nor contraband, its discovery promotes the objective of the border search exception to control who enters the country.

C. The Challenges to Applying Riley *and* Carpenter

Those arguing that *Riley* and *Carpenter* should inform the future handling of border searches of electronic devices face three challenges.[215] First, the Fourth Amendment's balancing test favors the government more at the border than it does anywhere else.[216] Second, searching electronic devices at the border advances the government interests that underlie the border search exception, unlike in *Riley*, where searches of cell phones did not advance the purposes of the search incident to arrest exception.[217] Finally, *Riley* and *Carpenter* both deal specifically with cell phones, not electronic devices, more broadly.[218]

Fourth Amendment balancing at the border is different from Fourth Amendment balancing elsewhere.[219] Indeed, searches in the interior that would be unconstitutional without a warrant are often permissible at the border without reasonable suspicion.[220] The Supreme Court has repeatedly recognized that the government's interests are at their peak at the border.[221] Conversely, the Supreme Court has repeatedly recognized that privacy interests are at their nadir at the border.[222] The unique balance of interests at the border precludes the blind application of the Fourth Amendment doctrine used in the interior at the border.

One rationale underlying the *Riley* holding is the Court's finding that the justifications for the search incident to arrest exception to the Fourth Amendment's warrant requirement are not implicated by searches of electronic devices.[223] Despite assertions to the contrary,

---

215. *See* Carpenter v. United States, 138 S. Ct. 2206 (2018); Riley v. California, 573 U.S. 373 (2014).

216. United States v. Montoya de Hernandez, 473 U.S. 531, 539–40 (1985) ("[T]he Fourth Amendment balance between the interests of the Government and the privacy right of the individual is . . . struck much more favorably to the Government at the border.").

217. *Supra* notes 49–55 and accompanying text.

218. *Carpenter*, 138 S. Ct. at 2211; *Riley*, 573 U.S. at 378.

219. *See Montoya de Hernandez*, 473 U.S. at 539–40.

220. *See, e.g.*, United States v. Flores-Montano, 541 U.S. 149, 155–56 (2004) (permitting searches of a vehicle's gas tank with no individualized suspicion).

221. *See, e.g.*, *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."); *supra* note 216.

222. *See, e.g.*, *Flores-Montano*, 541 U.S. at 154 ("[T]he expectation of privacy is less at the border than it is in the interior."); *supra* note 216.

223. *Supra* notes 49–55 and accompanying text.

searches of electronic devices do implicate the border search exception's underlying motivations.[224] The government has a strong interest in controlling who and what enters the country.[225] Searches of electronic devices contribute to the discovery of contraband, evidence of contraband, and evidence related to a noncitizen's admissibility.[226]

Riley and *Carpenter* both decided questions explicitly related to cell phones.[227] However, these are not the only electronic devices that CBP and ICE encounter at the border.[228] Both agencies' policies allow them to search a variety of electronic devices other than cell phones.[229] Published agency statistics do not break down searches by type of electronic device, but it is reasonable to assume that some of the thousands of searches that officers conduct are of devices besides cell phones.[230]

Riley, the more pertinent of the cases discussed in this Section, rests on two prongs.[231] The first is the unique privacy interests implicated by cell phones.[232] The second is the poor fit between (a) the purposes underlying the search incident to arrest exception to the Fourth Amendment's warrant requirement and (b) the results of cell phone searches incident to arrest.[233] In the border search context, privacy interests are weighed very differently from other situations.[234] Furthermore, cell phone searches strongly implicate the purposes of the border search exception.[235] Finally, border officials deal with many devices besides cell phones, and a one-size-fits-all approach to the

224. *Supra* note 141 and accompanying text.

225. *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."); United States v. Ramsey, 431 U.S. 606, 620 (1977) ("The border-search exception is grounded in the recognized right of the sovereign to control . . . who and what may enter the country.").

226. Alasaad v. Mayorkas, 988 F.3d 8, 21 (1st Cir. 2021) ("Advanced border searches of electronic devices may be used to search for contraband, evidence of contraband, or for evidence of activity in violation of the laws enforced or administered by CBP or ICE.").

227. Riley v. California, 573 U.S. 373, 378 (2014); Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

228. *See, e.g.*, CBP DIRECTIVE, *supra* note 16, at 2 (defining electronic device to include "computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players"); ICE DIRECTIVE, *supra* note 16, at 2 (using the same definition for electronic device as the CBP Directive).

229. *Supra* note 228.

230. CBP FY17 STATISTICS, *supra* note 11 ("In FY17, CBP conducted 30,200 border searches . . . "); *CBP Enforcement Statistics Fiscal Year 2021*, *supra* note 2 (indicating that CBP conducted 32,038 searches of electronic devices in FY 2020).

231. *Riley*, 573 U.S. at 385–86.

232. *Id.*

233. *Id.*

234. *Supra* note 216.

235. *See supra* notes 193–213 and accompanying text.

variety of electronic devices risks treating other devices as though they carry the same privacy implications as cell phones.[236] Because both prongs of the *Riley* decision are more favorable to the government at the border and border searches of electronics include devices besides cell phones, *Riley*'s warrant requirement should not be transferred to border searches.[237]

D. Real-World Impacts of This Solution

The effects of imposing a nationwide standard eschewing a reasonable suspicion requirement and allowing searches for more than contraband would be limited. The proposed standard will ease the administrability of these searches by reducing the number of "cookie-cutter" warrant applications for electronic device searches. It will also set a clear constitutional floor, from which Congress can legislate increased protections as technology evolves.

A holding creating a nationwide standard that requires no individualized suspicion for searches of electronic devices at the border, and allows searches for more than just contraband, is unlikely to change the number of searches for two reasons. First, the government is limited in the number of searches it can carry out as a practical matter. Second, the executive branch is incentivized to limit controversial searches as a policy matter to avoid imposing new statutory limits.

The government's finite resources naturally limit how many searches government officials can conduct.[238] On average, more than one million people enter the United States each day and must be processed by border officials.[239] This naturally limits the amount of time the government can spend scrutinizing each traveler. Just as the government does not have the time nor resources to inspect every vehicle that crosses a port of entry, it also cannot inspect more than a small percentage of the electronic devices that cross the border. If technological advancements change this reality, Congress can regulate when and how officers search electronic devices, or the executive branch can restrain itself through regulations.

Due to the looming possibility of federal legislation, CBP and ICE are incentivized to avoid controversy by self-regulating. One criticism of border searches of electronic devices is that officers and agents may target individuals for searches without a law enforcement

236. *See supra* note 228.

237. *See Riley*, 573 U.S. 373.

238. Today, less than .1% of border-crossers have their electronic devices searched. *Supra* notes 1–2 and accompanying text.

239. *Supra* note 1.

justification.[240] Both CBP and ICE already have policy limitations that require reasonable suspicion for advanced searches, even though some circuits do not require it.[241] Congress and the President are responsive to public pressure, and border searches of electronic devices have received coverage in various media outlets.[242] This attention pushes CBP and ICE to restrain themselves to avoid external limitations from Congress or the President.[243]

240. *E.g.*, Alasaad v. Nielsen, No. 17-CV-11730-DJC, 2018 WL 2170323, at *5 (D. Mass. May 9, 2018) (alleging CBP supervisor told plaintiffs he ordered a search of their cell phones because he "felt like" doing so). The plaintiffs in *Alasaad* also raised several other concerns. *Id.* at *5–8. Some of the plaintiffs alleged that allowing male CBP agents to view photos on their electronic devices of the plaintiffs without their religious headscarves violated the plaintiffs' religious beliefs. *Id.* at *5, *7, *22. Another plaintiff alleged CBP agents viewed privileged communications between attorney and client contained on his phone. Alasaad v. Nielsen, 419 F. Supp. 3d 142, 149–50 (D. Mass. 2019); *see also* Ashcroft v. Iqbal, 556 U.S. 662, 664 (2009) (discussing the federal government's response to the 9/11 attacks and stating "it is not surprising that a legitimate policy directing law enforcement to arrest and detain individuals because of their suspected link to the attacks would produce a disparate, incidental impact on Arab Muslims"). *But see CBP Policy on Nondiscrimination in Law Enforcement Activities and All Other Administered Programs*, U.S. CUSTOMS & BORDER PROT., https://www.cbp.gov/about/eeo-diversity/policies/nondiscrimination-law-enforcement-activities-and-all-other-administered [https://perma.cc/G7GK-U9XN] (Feb. 24, 2020) ("It is the policy of [CBP] to prohibit the consideration of race or ethnicity in law enforcement, investigation, and screening activities, in all but the most exceptional circumstances."); CBP DIRECTIVE, *supra* note 16, at 1 ("CBP will protect the rights of individuals against unreasonable search and seizure and ensure privacy protections while accomplishing its enforcement mission."); ICE DIRECTIVE, *supra* note 16, at 2–3 (requiring Special Agents in Charge ensure all agents they supervise complete required "training programs relevant to border searches of electronic devices, including constitutional, privacy, civil rights, and civil liberties training related to such searches").

241. *Supra* notes 26–27 and accompanying text.

242. Cristina M. Rodríguez, *Constraint Through Delegation: The Case of Executive Control over Immigration Policy*, 59 DUKE L.J. 1787, 1804, 1807 (2010); *see, e.g.*, Matthew S. Schwartz, *ACLU: Border Agents Violate Constitution when They Search Electronic Devices*, NPR (May 2, 2019, 5:10 AM), https://www.npr.org/2019/05/02/719337356/aclu-border-agents-violate-constitution-when-they-search-electronic-devices [https://perma.cc/JW3K-53XL]; Ron Nixon, *Cellphone and Computer Searches at U.S. Border Rise Under Trump*, N.Y. TIMES (Jan. 5, 2018) https://www.nytimes.com/2018/01/05/us/politics/trump-border-search-cellphone-computer.html [https://perma.cc/WQ6V-CEHR].

243. In fall 2021, a bipartisan group of Senators introduced a bill to limit border searches of electronic devices. Chris Mills Rodrigo, *Lawmakers Introduce Bill to Limit Data Collection at Border Crossings*, THE HILL (Oct. 7, 2021, 3:21 PM), https://thehill.com/policy/technology/575806-lawmakers-introduce-bill-to-limit-data-collection-at-border-crossings [https://perma.cc/96F2-NUSH]. The principal architects of the bill were Democratic Senator Ron Wyden of Oregon and Republican Senator Rand Paul of Kentucky. *Id.*

IV. CONCLUSION

The border search exception to the Fourth Amendment's warrant requirement dates back almost to the adoption of the amendment itself and is crucial to safeguarding the United States by controlling who and what crosses the border.[244] As times have changed, so have the types of contraband that cross the border and the ways in which they are concealed.[245] In recent years, various courts have grappled with the question of how to apply the border search exception to electronic devices.[246] Different circuits have come to different conclusions; some treat electronic devices like other types of property and allow searches without reasonable suspicion, while others require reasonable suspicion.[247] In *Cano*, the Ninth Circuit did even more by requiring reasonable suspicion that an electronic device contains contraband in order for officers to search it under the border search exception.[248]

It is time for the Supreme Court to weigh in, something it declined to do in 2021 despite ample opportunity.[249] The Supreme Court should hold that no reasonable suspicion is required for border searches of electronic devices.[250] The Court should also address and reject the Ninth Circuit's limitations on border searches imposed in *Cano*.[251] Border searches of electronic devices further the purposes of the border search exception—to control who and what enters the United States.[252] Searches do this by discovering contraband *and* evidence of contraband and evidence of a person's admissibility to the United States.[253] Rejecting *Cano* and allowing searches without reasonable suspicion will provide a constitutional floor upon which Congress can legislate additional protections as needed.[254] Congress is better situated to craft rules regulating privacy in evolving technology, and the Supreme Court should leave Congress the room to do so.[255] A holding by the Supreme Court that no reasonable suspicion is necessary for border searches of

244. *Supra* Sections I.A, I.C.
245. *Supra* Introduction.
246. *Supra* Section II.A.
247. *Supra* Section II.A.
248. *Supra* Section II.A.1.
249. *Supra* Section II.C.
250. *Supra* Section III.A.
251. *Supra* Section III.B.
252. *Supra* Section III.B.
253. *Supra* Section III.B.
254. *Supra* Section III.A.
255. *Supra* Section III.A.

electronic devices is unlikely to lead to major changes in the number or nature of searches, but will provide the necessary uniformity for agencies like CBP and ICE to operate.[256]

Davis Price Shugrue[*]

256. *Supra* Section III.D.

* JD Candidate, Vanderbilt University Law School, 2023; BS, Vanderbilt University, 2020. The Author would like to thank Nick Zotos and Professors Christopher Slobogin and Michael Bess for their insight and inspiration. He would also like to thank his parents and sister for their unwavering support, Professor Thomas Schwartz for his mentorship over many years, and Chandler Gerard-Reimer and the rest of the editorial staff of the *Vanderbilt Journal of Entertainment & Technology Law*. Finally, the Author would like to thank the many mentors and role models from his time at HRVLD and the CCSAO; there are too many to name individually, but all were invaluable role models and resources.