

WHERE DOES THE BORDER BEGIN AND THE FOURTH AMENDMENT END? WARRANTLESS FORENSIC SEARCHES OF OUTBOUND TRAVELERS’ ELECTRONIC DEVICES

ROBERT C. BUSCHEL, ESQ.*
BRADFORD M. COHEN, ESQ.**

I. INTRODUCTION 144

II. THE FOURTH AMENDMENT AND ITS CORE PROTECTIONS..... 146

III. THE BORDER SEARCH EXCEPTION: ORIGINS AND TRADITIONAL JUSTIFICATIONS..... 147

 A. *Historical Foundations in the First Congress*..... 147

 B. *Supreme Court Articulation: Entry as the Touchstone*..... 148

 C. *Traditional Justifications: Sovereignty, Contraband Prevention, and Security*..... 148

 D. *The Routine/Nonroutine Distinction*..... 149

IV. THE DIGITAL REVOLUTION AND ELECTRONIC PRIVACY 149

 A. *Riley v. California: Cell Phones as Categorically Different* 149

 B. *The “Resting on Its Own Bottom” Framework*..... 150

 C. *Carpenter v. United States: Digital Location Data* 151

V. WHAT HAPPENS TO KATZ, CARPENTER, AND RILEY AT THE BORDER? 152

 A. *The Circuit Split: Eleventh Circuit’s Categorical Approach* 152

 B. *The Fourth Circuit’s Reasonable Suspicion Standard*..... 153

 C. *The Ninth Circuit’s Contraband-Detection Limitation*..... 153

 D. *Other Circuits and District Courts* 154

VI. THE OUTBOUND TRAVELER PROBLEM: UNITED STATES V. GUMBS. 155

 A. *The Outbound Traveler Distinction*..... 155

 B. *Geographic and Temporal Displacement*..... 156

 C. *The Investigative Purpose Problem*..... 157

* Robert C. Buschel is a Partner at Buschel Gibbons, P.A., Fort Lauderdale, Florida. He is a member of the Bars of Florida and California. He focuses his practice on criminal defense, civil litigation, and appeals in state and federal court. He served as an editor of the Nova Law Review from 1994-95. He is also the author of two novels, *God’s Ponzi* (2022) and *By Silent Majority* (2016).

** Bradford M. Cohen is a Partner at Cohen & McMullen, P.A., Fort Lauderdale, Florida. A trial attorney with more than twenty-five years of experience, in State and Federal trials, barred in NY, FL, DC and Puerto Rico. He is a past President of the Broward County Association of Criminal Defense Lawyers, a member of the Million Dollar Verdict Club, and a graduate of Nova Southeastern University Shepard Broad College of Law (J.D. 1997).

VII.	ROUTINE VERSUS NON-ROUTINE SEARCHES AND ELECTRONIC DEVICES.....	158
A.	<i>The Inadequacy of Physical Analogies</i>	158
B.	<i>The Nature of Forensic Searches</i>	158
C.	<i>Time and Place Considerations</i>	159
VIII.	RECONCILING: A FRAMEWORK FOR ELECTRONIC DEVICE SEARCHES AT THE BORDER.....	160
A.	<i>The Inapplicability to Outbound Travelers</i>	160
B.	<i>Forensic Searches Require Reasonable Suspicion at Minimum</i>	160
C.	<i>The Warrant Requirement as the Better Rule</i>	161
D.	<i>First Amendment Considerations</i>	162
IX.	CONCLUSION.....	162

I. INTRODUCTION

Before you board, please hand your cellphone and laptop computer to a Customs and Border Protection Agent and it will be returned to you after data-extraction.

U.S. agents do not seize every device from travelers before they leave the country, for one reason, because current technology cannot efficiently download and sort electronic device data.¹ However, warrantless seizures and off-site searches of electronic data for generalized law enforcement purposes are expanding in the name of notorious crimes like human trafficking, child pornography, and gun and drug running.² There is a border exception to the warrant requirement of the Fourth Amendment.³ Further, case law has expanded the border to mean the “functional equivalent” of the border.⁴ What if one is leaving the country from Miami or Boise to travel to Paris? When does the traveler cross the border? How long may government agents seize electronic equipment and search it? What level of suspicion is required before agents can search electronic equipment at the border? These answers depend on what is the point of departure or entry in the United States and the purpose of the search relates to border protection versus other generalized law enforcement goals.

The Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and

1. See *United States v. Kolsuz*, 890 F.3d 133, 139, 145 (4th Cir. 2018).

2. See *id.* at 137, 142, 144; *United States v. Gumbs*, 799 F. Supp. 3d 1252, 1255 (S.D. Fla. 2025).

3. *The Border Search Muddle*, 132 HARV. L. REV. 2278, 2278, 2280 (2019).

4. *Kolsuz*, 890 F.3d at 137.

seizures”⁵ This fundamental protection, however, encounters its most significant limitation at the nation’s borders. The border search exception to the Fourth Amendment permits warrantless searches at international boundaries based on sovereignty principles traced to the First Congress.⁶ Yet recent technological developments have created a constitutional setback: the collision between this historical exception and the modern reality of electronic devices that contain “the privacies of life.”⁷

The question is no longer merely academic. Circuit courts have fractured on whether the border search exception extends to forensic searches of outbound travelers’ cell phones seized for criminal investigative purposes unrelated to border security.⁸ The Eleventh Circuit’s categorical language in *United States v. Vergara*⁹ and *United States v. Touse*,¹⁰ that border searches “never require probable cause or a warrant”¹¹ collides with the Fourth Circuit’s post-*Riley* framework requiring reasonable suspicion for forensic device searches.¹² *United States v. Gumbs*,¹³ represents the first published Southern District of Florida decision addressing whether the exception applies when: (1) the traveler is departing, not entering the country; (2) the seizure occurs at a U.S. airport, not the physical border; (3) the forensic search occurs weeks later in a different state; and (4) the government seeks evidence of past criminal conduct, not contraband.¹⁴

This article asserts the border search exception should not extend to these circumstances. The digital revolution demands constitutional update. When Judge Learned Hand wrote that searching a man’s pockets differs fundamentally from “ransacking his house for everything which may incriminate him,”¹⁵ he may not have imagined that those pockets would one day carry devices containing years of intimate communications and photographs, location history and path tracking, and personal financial and health data. Cell phones are no longer “another technological convenience;” they are repositories of digital life.¹⁶ It is nigh time for our judicial system to recognize that our electronic devices are the functional equivalent of our

5. U.S. CONST. amend. IV.

6. See *United States v. Ramsey*, 431 U.S. 606, 619 (1977).

7. See *Riley v. California*, 573 U.S. 373, 403 (2014).

8. See *United States v. Vergara*, 884 F.3d 1309, 1317 (11th Cir. 2018); *United States v. Touse*, 890 F.3d 1227, 1229, 1230 (11th Cir. 2018); *Kolsuz*, 890 F.3d at 143.

9. 884 F.3d 1309 (11th Cir. 2018).

10. 890 F.3d 1227 (11th Cir. 2018).

11. *Id.* at 1232; *Vergara*, 884 F.3d at 1312.

12. See *Kolsuz*, 890 F.3d at 146.

13. 799 F. Supp. 3d 1252 (S.D. Fla. 2025).

14. See *id.* at 1255.

15. *United States v. Kirschenblatt*, 16 F.2d 202, 203 (2d Cir. 1926).

16. *Riley v. California*, 573 U.S. 373, 403, 407 (2014).

“houses, papers, and effects” contemplated by the text of the Fourth Amendment.

II. THE FOURTH AMENDMENT AND ITS CORE PROTECTIONS

The Fourth Amendment establishes a baseline requirement: searches and seizures must be reasonable.¹⁷ The “ultimate touchstone” of Fourth Amendment analysis remains reasonableness, measured through a careful balancing of governmental interests against individual privacy expectations.¹⁸ When law enforcement seeks to discover evidence of criminal wrongdoing, reasonableness generally requires a judicial warrant supported by probable cause.¹⁹ The warrant requirement interjects a “neutral and detached magistrate” between citizens and “the competitive enterprise of ferreting out crime.”²⁰

The Amendment’s text explicitly protects “persons, houses, papers, and effects.”²¹ This enumeration reflects Founding-era concerns about general warrants and writs of assistance that permitted officials to search anywhere for anything.²² The protection for “papers” holds particular significance for this analysis, as it demonstrates the Framers’ specific concern with documentary evidence and the privacy interests implicated by its review.²³

Fourth Amendment doctrine recognizes that “the Fourth Amendment protects people, not places.”²⁴ Under *Katz v. United States*,²⁵ a search occurs when the government violates a person’s reasonable expectation of privacy.²⁶ This two-part test asks whether the individual manifested a subjective expectation of privacy and whether society recognizes that expectation as objectively reasonable.²⁷ “A person does not surrender all Fourth Amendment protection by venturing into the public sphere.”²⁸ Even in areas accessible to

17. See U.S. CONST. amend. IV.

18. See *Riley*, 573 U.S. at 381, 407.

19. See *id.* at 381, 382.

20. *Id.* at 382 (quoting *Johnson v. United States*, 333 U.S. 10, 14 (1948)).

21. U.S. CONST. amend. IV.

22. See Donald A. Dripps, “Dearest Property”: *Digital Evidence and the History of Private “Papers” as Special Objects of Search and Seizure*, 103 J. CRIM. L. & CRIMINOLOGY 49, 61 (2013).

23. See *id.* at 106.

24. *Katz v. United States*, 389 U.S. 347, 351 (1967).

25. 389 U.S. 347 (1967).

26. *Id.* at 353, 361 (Harlan, J., concurring).

27. *Id.* at 361 (Harlan, J., concurring).

28. *Carpenter v. United States*, 585 U.S. 296, 310 (2018).

the public, “what [one] seeks to preserve as private . . . may be constitutionally protected.”²⁹

III. THE BORDER SEARCH EXCEPTION: ORIGINS AND TRADITIONAL JUSTIFICATIONS

The border search exception permits warrantless searches at international boundaries without individualized suspicion.³⁰ The Supreme Court has described this exception as “as old as the Fourth Amendment itself.”³¹ In *United States v. Ramsey*,³² the Court explained that “searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border.”³³

A. *Historical Foundations in the First Congress*

Courts frequently cite the First Congress’s enactment of the Collection Act of 1789 as evidence of the border exception’s constitutional pedigree.³⁴ This statute authorized customs officers to board and search “any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to dut[ies]. . . .”³⁵ The Eleventh Circuit in *Touset* emphasized that “[t]he First Congress—the same one that proposed the Fourth Amendment—empowered customs officials to stop and search without a warrant any vessel or cargo suspected of illegally entering our nation.”³⁶

However, this historical narrative deserves closer scrutiny. As Professor William Cuddihy observed, “the most obvious indices of [original] meaning [are] few and uninformative”³⁷ “[T]he Collection Act speaks only to ‘goods, wares and merchandise.’”³⁸ “It says nothing about papers or their equivalent. . . .”³⁹ Critically, it does not authorize “obtain[ing] evidence

29. *Katz*, 389 U.S. at 351–52.

30. *United States v. Ramsey*, 431 U.S. 606, 619 (1977).

31. *Id.*

32. 431 U.S. 606 (1977).

33. *Id.* at 616.

34. *See, e.g.*, *United States v. Touset*, 890 F.3d 1227, 1232 (11th Cir. 2018).

35. Act of July 31, 1789, ch. 5, § 24, 1 Stat. 29, 43 (repealed 1790).

36. *Touset*, 890 F.3d at 1232.

37. *The Border Search Muddle*, *supra* note 3, at 2289.

38. *Id.* at 2293.

39. *Id.*

of crimes other than the contraband itself.”⁴⁰ The historical evidence supporting the border exception addresses incoming contraband, not outgoing travelers or investigative evidence-gathering.⁴¹

B. *Supreme Court Articulation: Entry as the Touchstone*

Every Supreme Court decision invoking the border search exception has involved persons or items entering the United States.⁴² In *United States v. Ramsey*, the Court stated that “[b]order searches, then, from before the adoption of the Fourth Amendment, have been considered to be ‘reasonable’ by the single fact that the person or item in question had entered into our country from outside.”⁴³ The Court’s deliberate use of “entered” and “single fact” language “supports the proposition that a border search would not automatically be deemed reasonable if the person or item had not entered into the country from outside.”⁴⁴

C. *Traditional Justifications: Sovereignty, Contraband Prevention, and Security*

The border search exception rests on three interconnected justifications. First, the federal government possesses the sovereign right to control “who and what may enter the country.”⁴⁵ Second, the government maintains a heightened interest in preventing the introduction of contraband, “whether that be communicable diseases, narcotics, or explosives.”⁴⁶ Third, the government must protect national security by monitoring and regulating international entry points.⁴⁷

These justifications share a common theme: they focus overwhelmingly on inbound travel and the detection of incoming threats.⁴⁸ The purpose of a border search is to collect duties and prevent the introduction of contraband into the country.⁴⁹ This directional emphasis appears repeatedly in Supreme Court of the United States border search jurisprudence.⁵⁰

40. *Id.*

41. *See id.* at 2293, 2294.

42. *United States v. Gumbs*, 799 F. Supp. 3d 1252, 1256 (S.D. Fla. 2025).

43. *Id.* at 619.

44. *Gumbs*, 799 F. Supp. 3d at 1257.

45. *Ramsey*, 431 U.S. at 620.

46. *See United States v. Montoya de Hernandez*, 473 U.S. 531, 544 (1985).

47. *See Ramsey*, 431 U.S. at 618, 619.

48. *See Gumbs*, 799 F. Supp. 3d at 1257.

49. *See Montoya de Hernandez*, 473 U.S. at 537.

50. *See Ramsey*, 431 U.S. at 616, 619.

D. *The Routine/Nonroutine Distinction*

Not all border searches receive identical treatment. Courts distinguish between “routine” searches requiring no suspicion and “nonroutine” searches that demand reasonable suspicion.⁵¹ In *United States v. Montoya de Hernandez*,⁵² the Supreme Court of the United States held that the prolonged detention of a suspect believed to be carrying narcotics in her alimentary canal was “beyond the scope of a routine customs search” and required some level of suspicion.⁵³ The Eleventh Circuit has similarly held that “highly intrusive searches of a person’s body such as a strip search or an x-ray examination” are likewise nonroutine and thus require reasonable suspicion.⁵⁴

Yet, the Supreme Court of the United States has left crucial questions unanswered: “whether, and under what circumstances, a border search might be deemed ‘unreasonable’ because of the particularly offensive manner in which it is carried out.”⁵⁵ The Court has suggested that “in the case of highly intrusive searches” where salient “dignity and privacy interests” are at stake, a requirement of suspicion might be supported.⁵⁶ This analytical framework takes on new significance when applied to forensic searches of electronic devices.

IV. THE DIGITAL REVOLUTION AND ELECTRONIC PRIVACY

A. *Riley v. California: Cell Phones as Categorically Different*

In 2014, the Supreme Court of the United States unanimously held in *Riley v. California*⁵⁷ that police generally must obtain a warrant before searching a cell phone seized incident to arrest.⁵⁸ Chief Justice Roberts’s opinion recognized the unique privacy interests implicated by cell phone searches, noting that modern devices contain “the privacies of life” and that “[t]he sum of an individual’s private life can be reconstructed” through their contents.⁵⁹

51. See, e.g., *Montoya de Hernandez*, 473 U.S. at 538, 541.

52. 473 U.S. 531 (1985).

53. *Id.* at 541.

54. *United States v. Alfaro-Moncada*, 607 F.3d 720, 729 (11th Cir. 2010); see *Gilmore v. Ga. Dep’t of Corr.*, 144 F.4th 1246, 1254 (11th Cir. 2025) (finding reasonable suspicion required that visitor in prison is concealing contraband before strip-search).

55. *United States v. Flores-Montano*, 541 U.S. 149, 155 n.2 (2004) (quoting *Ramsey*, 431 U.S. at 618 n.13).

56. *Id.* at 152.

57. 573 U.S. 373 (2014).

58. *Id.* at 403.

59. *Id.* at 394, 403.

The Court rejected the government's argument that cell phones should receive no special treatment.⁶⁰ *Riley* emphasized both quantitative and qualitative differences. Quantitatively, cell phones can store millions of pages of text, thousands of pictures, or hundreds of videos.⁶¹ Qualitatively, they contain types of information—browsing history, location data, and private conversations that would have been too burdensome to carry in physical form.⁶² A search of a cell phone “would typically expose to the government far *more* than the most exhaustive search of a house”⁶³ Indeed, some people would sooner have a government agent search their house rather than their phone.

The Court observed that “[m]odern cell phones are not just another technological convenience”; a visitor from Mars might conclude they “were an important feature of human anatomy.”⁶⁴ Cell phones differ from physical containers because they provide access to information about “familial, political, professional, religious, and sexual associations” through contact lists, text messages, and browsing history.⁶⁵ The Court concluded that “‘privacy-related concerns are weighty enough’ [that] a ‘search may require a warrant, notwithstanding the diminished expectations of privacy’”⁶⁶ These findings demonstrate a leap in the Court’s technological knowledge and ubiquity of mobile communication from four years earlier.⁶⁷

B. *The “Resting on Its Own Bottom” Framework*

Riley established a crucial analytical principle: when extending a warrant exception to new contexts, courts must ensure the exception “rest[s] on its own bottom.”⁶⁸ The Court framed the relevant question as whether applying an exception to digital devices would “untether the rule from the justifications underlying [it]”⁶⁹ This framework demands that each

60. *See id.* at 393.

61. *See id.* at 393, 394.

62. *Riley*, 573 U.S. at 394, 395.

63. *Id.* at 396.

64. *Id.* at 385, 403.

65. *Id.* at 379, 396, 397 (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

66. *Id.* at 392 (quoting *Maryland v. King*, 569 U.S. 435, 463 (2013)).

67. *See Riley*, 573 U.S. at 392; Transcript of Oral Argument at 29, *City of Ontario v. Quon*, 560 U.S. 746 (2010) (No. 08–1332) (“CHIEF JUSTICE ROBERTS: Maybe - maybe everybody else knows this, but what is the difference between the pager and the e-mail?”).

68. *Riley*, 573 U.S. at 393.

69. *See id.* at 386 (quoting *Arizona v. Gant*, 556 U.S. 332, 343 (2009)).

warrant exception justify its own extension to cell phone searches based on its particular purposes.

The Court rejected the government's categorical approach, which would have permitted cell phone searches simply because searches incident to arrest were historically allowed.⁷⁰ Instead, *Riley* required courts to examine whether the rationales underlying a particular exception, officer safety and evidence preservation for searches incident to arrest, applied with equal force to digital devices.⁷¹ Finding they did not, the Court required warrants for cell phone searches even for arrestees with diminished privacy expectations.⁷²

C. *Carpenter v. United States: Digital Location Data*

Four years later, *Carpenter v. United States*⁷³ extended *Riley*'s principles to cell site location information ("CSLI").⁷⁴ The Court held that individuals maintain a legitimate expectation of privacy in the record of their physical movements as captured through CSLI.⁷⁵ Chief Justice Roberts explained that "'when privacy-related concerns are weighty enough[,] a 'search may require a warrant.'"⁷⁶

Carpenter rejected the third-party doctrine's application to digital location data,⁷⁷ because "allowing the [government] to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case."⁷⁸ Modern technology generates "a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."⁷⁹

70. *Id.* at 403.

71. *See id.* at 386, 387.

72. *Id.* at 403.

73. 585 U.S. 296 (2018).

74. *See id.* at 305–06, 310.

75. *See id.* at 310.

76. *Riley*, 573 U.S. at 392 (quoting *Maryland v. King*, 569 U.S. 435, 463 (2013)).

77. *Carpenter*, 585 U.S. at 309; *United States v. Miller*, 425 U.S. 435, 443 (1976) (The third-party doctrine under the Fourth Amendment does not prohibit the obtaining of information revealed to a *third party* to government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed).

78. *Riley*, 573 U.S. at 395.

79. *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

Together, *Riley* and *Carpenter* establish that digital information receives heightened Fourth Amendment protection based on the quantity, quality, and intimacy of data modern devices contain and generate.⁸⁰

V. WHAT HAPPENS TO *KATZ*, *CARPENTER*, AND *RILEY* AT THE BORDER?

If a traveler brings a cell phone to the border, can it be seized and searched elsewhere any time later? Does a purported international traveler lose all reasonable expectation of privacy in one's pre-travel life (in digital form) simply by attempting to board an international flight, boat, or train? What happens to the holdings of *Katz*, *Carpenter*, and *Riley* at the border?

A. *The Circuit Split: Eleventh Circuit's Categorical Approach*

The Eleventh Circuit has adopted the most permissive standard for border searches of electronic devices.⁸¹ In *Vergara*, the court held that "[b]order searches 'never' require probable cause or a warrant."⁸² Judge William Pryor's opinion emphasized the "impressive historical pedigree" of border searches and concluded that the government need not obtain a warrant before conducting forensic searches of cell phones at the border.⁸³

The majority explicitly rejected *Riley's* application to the border context, reasoning that *Riley* "expressly limited its holding" to the search-incident-to-arrest exception.⁸⁴ The court concluded that forensic searches of electronic devices at the border require neither a warrant nor probable cause.⁸⁵ *United States v. Touset* followed *Vergara*, reiterating that "no suspicion is necessary to search electronic devices at the border."⁸⁶

Judge Jill Pryor dissented in *Vergara*, stating that the majority's categorical approach ignored the unique privacy interests *Riley* recognized.⁸⁷ In her dissent, she conducted a balancing test between the government's "heightened interest at the border" and the privacy interest in cell phone data,

80. See *Riley*, 573 U.S. at 403; *Carpenter*, 585 U.S. at 320.

81. See *United States v. Vergara*, 884 F.3d 1309, 1313, 1315 (11th Cir. 2018) (Pryor, J., dissenting) (qualifying as the "most permissive" because the majority's opinion is one that "weighs heavily in the government's favor" and dismisses "significant privacy interests" by favoring the government over the individual's Fourth Amendment rights, which the 9th Circuit strayed away from).

82. *Id.* at 1312.

83. *Id.* at 1312, 1313.

84. *Id.* at 1312.

85. *Id.*

86. *United States v. Touset*, 890 F.3d 1227, 1229 (11th Cir. 2018).

87. See *Vergara*, 884 F.3d at 1313 (Pryor, J., dissenting).

concluding that privacy interests prevailed.⁸⁸ Judge Pryor argued that forensic searches of cell phones at the border require probable cause and a warrant, noting that “forensic searches” are qualitatively different from “manual searches.”⁸⁹

B. *The Fourth Circuit’s Reasonable Suspicion Standard*

The Fourth Circuit charted a different course in *United States v. Kolsuz*.⁹⁰ In stark contrast to the Eleventh Circuit, the Court held that forensic border searches of digital devices must be treated as nonroutine, permissible only on a showing of individualized suspicion.⁹¹ The court reasoned that Riley recognized that electronic devices “implicate privacy concerns far beyond those implicated” by other physical objects.⁹²

Kolsuz established that “[a]fter Riley, we think it is clear that a forensic search of a digital phone must be treated as a nonroutine border search, requiring some form of individualized suspicion.”⁹³ The Fourth Circuit the following year clarified in *United States v. Aigbekaen*⁹⁴ that the required suspicion must have “some nexus to the purposes of the border search exception” before a warrantless forensic search is allowed.⁹⁵

Judge Wilkinson concurred in *Kolsuz* but objected that the court’s approach departed from “longstanding historical practice in border searches of deferring to the legislative and executive branches.”⁹⁶ He argued that determining the proper balance between privacy and security at the border was a question for the political branches, not courts.⁹⁷

C. *The Ninth Circuit’s Contraband-Detection Limitation*

The Ninth Circuit adopted yet another approach in *United States v. Cano*,⁹⁸ requiring reasonable individualized suspicion for forensic searches, but adding an important limitation.⁹⁹ The court held that the border search exception “authorizes warrantless searches . . . only to determine whether the

88. *Id.* at 1313, 1318.

89. *Id.* at 1315.

90. *United States v. Kolsuz*, 890 F.3d 133, 133 (4th Cir. 2018).

91. *Id.* at 143, 146.

92. *Id.* at 152.

93. *Id.* at 146.

94. 943 F.3d 713 (4th Cir. 2019).

95. *Id.* at 723.

96. *Kolsuz*, 890 F.3d at 153 (Wilkinson, J., concurring).

97. *Id.* at 148, 152–53.

98. 934 F.3d 1002 (9th Cir. 2019).

99. *Id.* at 1007.

phone contains contraband.”¹⁰⁰ This narrower interpretation prevents broader searches untethered from the exception’s purposes.¹⁰¹

Under *Cano*, reasonable suspicion must relate specifically to digital contraband.¹⁰² The court distinguished between manual searches, permitted without suspicion, and forensic examinations, requiring reasonable suspicion.¹⁰³ This framework recognizes that forensic searches constitute a “computer strip search” that demands heightened protection.¹⁰⁴

D. *Other Circuits and District Courts*

Several circuits have acknowledged the issue without definitively resolving it. The Fifth Circuit in *United States v. Castillo*¹⁰⁵ recognized that “government searches of [modern cell phones] have the potential to be uniquely intrusive,” distinguishing them from property traditionally subject to the border search exception.¹⁰⁶ However, the court did not reach the question of whether forensic searches require reasonable suspicion.¹⁰⁷

The Eighth Circuit in *United States v. Xiang*¹⁰⁸ expressed agreement with other circuits’ conclusions that “a forensic or ‘advanced’ search . . . becomes a nonroutine border search requiring some level of reasonable, individualized suspicion . . . given the heightened personal privacy interest in electronic devices recognized in *Riley*.”¹⁰⁹ In *United States v. Mendez*,¹¹⁰ the Seventh Circuit similarly noted that nonroutine searches require reasonable suspicion but declined to decide whether “intrusive, forensic electronic device searches” fall into that category.¹¹¹

Multiple district courts have gone further, requiring warrants for cell phone searches at the border. In *United States v. Smith*,¹¹² the Southern District of New York held that warrants are required for forensic border searches of electronic devices.¹¹³ The Eastern District of New York reached a similar

100. *Id.* at 1018.

101. *Id.*

102. *Id.* at 1007.

103. *Cano*, 934 F.3d at 1007.

104. *See United States v. Cotterman*, 709 F.3d 952, 966 (9th Cir. 2013).

105. 70 F.4th 894 (5th Cir. 2023).

106. *Id.* at 897.

107. *See id.* at 898.

108. 67 F.4th 895 (8th Cir. 2023).

109. *Id.* at 900–01.

110. 103 F.4th 1303 (7th Cir. 2024).

111. *Id.* at 1304, 1310.

112. 673 F. Supp. 3d 381 (S.D.N.Y. 2023).

113. *Id.* at 394.

conclusion in *United States v. Sultanov*,¹¹⁴ finding that forensic searches transform routine border searches into nonroutine searches requiring heightened protection—a warrant.¹¹⁵

VI. THE OUTBOUND TRAVELER PROBLEM: *UNITED STATES V. GUMBS*

United States v. Gumbs presents the border search exception’s most challenging application.¹¹⁶ In March 2024, federal agents seized three cell phones from Jeleel Gumbs as he attempted to board an international flight from Atlanta to St. Martin.¹¹⁷ The phones were then shipped to Miami and subjected to forensic examination two weeks later using specialized software.¹¹⁸ Through its search, the government sought evidence related to an alleged firearms export violation stemming from a seizure of firearms seventeen months earlier.¹¹⁹

The district court granted Gumbs’ motion to suppress on three independent grounds, each exposing fundamental problems with extending the border search exception to his circumstances.¹²⁰

A. *The Outbound Traveler Distinction*

Every Eleventh Circuit case applying the border search exception has involved *entrants* to the United States.¹²¹ The Supreme Court’s language in *Ramsey* emphasized that border searches “have been considered to be ‘reasonable’ by the single fact that the person or item in question had entered into our country from outside.”¹²² The Court’s intentional use of “entered” and “‘single fact’ clearly supports the proposition that a border search would not automatically be deemed reasonable if the person or item had not entered . . . from outside.”¹²³

“[N]one of the significant government interests in monitoring what *enters* the country applies where . . . the object of a warrantless border search

114. 742 F. Supp. 3d 258 (E.D.N.Y. 2024).

115. *Id.* at 288.

116. *See* *United States v. Gumbs*, 799 F. Supp. 3d 1252, 1255, 1256 (S.D. Fla. 2025).

117. *Id.* at 1254.

118. *Id.*

119. *See id.* at 1253–54.

120. *Id.* at 1255, 1260.

121. *Gumbs*, 799 F. Supp. 3d at 1255–56.

122. *United States v. Ramsey*, 431 U.S. 606, 619 (1977).

123. *Gumbs*, 799 F. Supp. 3d at 1257.

was [leaving] the country.”¹²⁴ Gumbs was not attempting to bring anything into the United States; he was an outbound traveler attempting to depart.¹²⁵ This distinction is critical because the traditional justifications for the border search exception—preventing contraband entry, enforcing immigration laws, and collecting duties—simply do not apply to departing travelers.¹²⁶

The Eleventh Circuit itself had recognized this distinction in *United States v. Hernandez-Salazar*,¹²⁷ where it narrowly held that Congress may authorize warrantless searches of persons departing the United States only “on the basis of reasonable suspicion that a currency reporting violation is occurring.”¹²⁸ Critically, this conclusion rested on explicit statutory authority Congress provided for currency violations.¹²⁹ No parallel broad search authority exists for forensic device searches of outbound travelers.¹³⁰

B. *Geographic and Temporal Displacement*

Gumbs’s phones were seized at Atlanta’s Hartsfield-Jackson International Airport, a “functional equivalent”¹³¹ of the border, but were transported to Miami and searched weeks later.¹³² The “border” has included entire metropolitan areas such as San Diego, El Paso, and the South Texas Rio Grande Valley.¹³³ This significant geographic and temporal displacement removes the search from the traditional border context.¹³⁴

In *United States v. Kim*,¹³⁵ the District Court for the District of Columbia found that a laptop search conducted away from the border and weeks after the initial seizure was so disconnected from the border itself that it could not be justified under the border search exception.¹³⁶ The court examined the traditional justifications for border searches and found them

124. *United States v. Kolsuz*, 185 F. Supp. 3d 843, 857–58 (E.D. Va. 2016), *aff’d*, 890 F.3d 133 (4th Cir. 2018).

125. *Gumbs*, 799 F. Supp. 3d at 1254, 1255.

126. *See id.* at 1255, 1257.

127. 813 F.2d 1126 (11th Cir. 1987).

128. *Id.* at 1138.

129. *Id.* at 1133, 1138; 31 U.S.C. § 5317(a)(b).

130. *See Gumbs*, 799 F. Supp. 3d at 1258.

131. *See id.* at 1254, 1257.

132. *Id.* at 1254.

133. *Students for Fair Admissions, Inc. v. President & Fellows of Harvard Coll.*, 143 S. Ct. 2141, 2246 (2023) (quoting *United States v. Brignoni-Ponce*, 422 U.S. 873, 882 (1975)).

134. *See id.*

135. 103 F. Supp. 3d 32 (D.D.C. 2015).

136. *Id.* at 59.

inapplicable where the search occurred approximately two weeks after seizure and 150 miles from the airport.¹³⁷

The *Gumbs* court similarly found that the two-week delay and the forensic search at the Miami location defeated any claim that the search occurred “at the border.”¹³⁸ This temporal and geographic displacement between seizure and search matters, because the border search exception rests on the immediate governmental interest in monitoring the border, not on creating a roving exception that follows travelers and their property indefinitely.¹³⁹

C. *The Investigative Purpose Problem*

Perhaps most distinctive, the forensic search of *Gumbs*’s phones served purely investigative purposes related to a dormant domestic criminal case rather than a search for contraband.¹⁴⁰ The government placed a “Look Out” on *Gumbs* not because of any border-related concern, but to gather evidence for a seventeen-month-old exportation of firearms investigation.¹⁴¹ This use of the border exception untethers it entirely from its historical and constitutional justifications.¹⁴²

The district court warned that “adopting an unconstrained view” of the border search exception “risks turning the border search doctrine into an invitation for abuse.”¹⁴³ Under the government’s theory, “[a]ny law enforcement agency could place a Look Out on a person for any reason, including personal animus or disagreement with protected speech, and wait until the person” attempts international travel.¹⁴⁴ “[L]aw enforcement could then gain full access to the person’s electronic devices and review the entire scope of their personal and professional history, without reasonable suspicion, probable cause, or ever having to justify the search to a neutral magistrate.”¹⁴⁵

This scenario conflicts fundamentally with Fourth Amendment protections, “a provision of the Constitution which sought to guard against an abuse that more than any one single factor gave rise to American

137. *See id.* at 35, 41.

138. *See United States v. Gumbs*, 799 F. Supp. 3d 1252, 1257 (S.D. Fla. 2025).

139. *See Kim*, 103 F. Supp. at 59.

140. *Gumbs*, 799 F. Supp. 3d at 1259–60.

141. *Id.* at 1254.

142. *See id.* at 1259.

143. *Id.*

144. *Id.*

145. *Gumbs*, 799 F. Supp. 3d at 1259.

independence.”¹⁴⁶ Allowing such searches would “untether” the exception “from the justifications underlying it.”¹⁴⁷

VII. ROUTINE VERSUS NON-ROUTINE SEARCHES AND ELECTRONIC DEVICES

A. *The Inadequacy of Physical Analogies*

The routine/nonroutine distinction developed in the context of physical searches of the person or a cursory search through luggage, as compared to a body cavity search, are distinct and obvious.¹⁴⁸ These categories become meaningless when applied to electronic devices. As the Fourth Circuit recognized, cell phones are not unlike “tractor-trailer[s] loaded with boxes,” they present both quantitative and qualitative differences from pre-digital searches.¹⁴⁹ Forensic searches of cell phones extract gigabytes of intimate data, the digital equivalent of every piece of mail, every picture taken, and every book or article a person has ever received or read.¹⁵⁰ Modern devices provide access to location history, communication patterns, deleted data, and metadata that reveal associations and activities.¹⁵¹ The ease with which this information can be extracted should not diminish the Fourth Amendment interests at stake.¹⁵²

B. *The Nature of Forensic Searches*

Forensic searches are not a simple pat down for weapons.¹⁵³ They generally entail the connection of external equipment and/or the use of specialized software such as Cellebrite¹⁵⁴ or Oxygen Forensics.¹⁵⁵ Homeland

146. *Id.* (quoting *Harris v. United States*, 331 U.S. 145, 159 (1947) (Frankfurter, J., dissenting)).

147. *Id.* (quoting *Collins v. Virginia*, 138 S. Ct. 1663, 1667 (2018)).

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

149. *See Riley v. California*, 573 U.S. 373, 393 (2014); *The Border Search Muddle*, *supra* note 3, at 2286 (quoting *United States v. Touset*, 890 F.3d 1227, 1235 (11th Cir. 2018)).

150. *Riley*, 573 U.S. at 393–94.

151. *See id.* at 394–95; *United States v. Kim*, 103 F. Supp. 3d 32, 50 (D.D.C. 2015).

152. *See Riley*, 573 U.S. at 403.

153. *See Kim*, 103 F. Supp. 3d at 51.

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

155. OXYGEN FORENSICS, <http://www.oxygenforensics.com/en/company/about-us/> [<http://perma.cc/2F63-Z4M5>] (last visited Apr. 9, 2026).

Security Investigations' Computer Forensic Analysis can extract and analyze data using such specialized tools.¹⁵⁶ These searches go far beyond the manual scrolling through a phone that might occur during a routine inspection.¹⁵⁷

The Ninth Circuit aptly characterized forensic searches as a "computer strip search."¹⁵⁸ They extract not only current data, but also deleted files, analyze communication patterns, and reconstruct a comprehensive picture of the device owner's life.¹⁵⁹ While not a physical intrusion of the body, forensic searches constitute a different type of invasiveness into the most private aspects of life.¹⁶⁰ The government's ability to conduct such searches may also be limited by the Fifth Amendment when compelling a traveler to disclose a password, which would constitute testimonial self-incrimination.¹⁶¹

C. *Time and Place Considerations*

Contemporaneous searches at the actual border differ fundamentally from delayed searches conducted hundreds of miles away.¹⁶² A two-week delay between seizure and search, combined with search location hundreds of miles away, defeat any claim that the search occurred at or near the border.¹⁶³ As the *Gumbs* court observed, in this case, the border has moved from the Northern District of Georgia to the Southern District of Florida.¹⁶⁴ If the border search exception permits such displacement, it ceases to be a border search exception at all; it becomes a warrant exception for any property seized near international travel, searchable at any time and place the government finds convenient.¹⁶⁵

156. See, e.g., *Kolsuz*, 185 F. Supp. at 849; *Kim*, 103 F. Supp. 3d at 40.

157. See *United States v. Cano*, 934 F.3d 1002, 1015, 1016 (9th Cir. 2019).

158. *Id.* at 1015.

159. See *United States v. Cotterman*, 709 F.3d 952, 957, 962–63, 964 (9th Cir. 2013).

160. *Kim*, 103 F. Supp. 3d at 50, 51.

161. Compare *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012) (compelling disclosure of device passwords may implicate the Fifth Amendment and protections against self-incrimination), and *Doe v. United States*, 487 U.S. 201, 213–14 (1988) (“[t]here are very few instances in which a verbal statement, either oral or written, will not convey information or assert facts. The vast majority of verbal statements thus will be testimonial and, to that extent at least, will fall within the privilege.”), with *United States v. Apple Mac Pro Comput.*, 851 F.3d 238, 248 (3d Cir. 2017) (applying “foregone conclusion” exception).

162. See *Kim*, 103 F. Supp. 3d at 57, 58.

163. *Id.*

164. *United States v. Gumbs*, 799 F. Supp. 3d 1252, 1254 (S.D. Fla. 2025).

165. See *id.* at 1257, 1258.

VIII. RECONCILING: A FRAMEWORK FOR ELECTRONIC DEVICE SEARCHES AT THE BORDER

A. *The Inapplicability to Outbound Travelers*

The border search exception should not apply to outbound travelers whose electronic devices are seized for investigative purposes unrelated to border security.¹⁶⁶ The traditional justifications—preventing contraband entry, enforcing immigration laws, and collecting duties—focus entirely on incoming threats.¹⁶⁷ These interests evaporate when the traveler is departing.¹⁶⁸

The statutory framework reinforces this distinction. Congress has explicitly authorized suspicion-less searches for currency reporting violations by outbound travelers under 31 U.S.C. § 5317.¹⁶⁹ The absence of similar statutory authority for forensic device searches suggests Congress did not intend the border search exception to extend so broadly.¹⁷⁰ In the instances where Congress has spoken specifically about outbound searches, it has required reasonable suspicion and limited the search to specific contraband.¹⁷¹

B. *Forensic Searches Require Reasonable Suspicion at Minimum*

Even if some border search authority extends to electronic devices of outbound travelers, forensic searches must be treated as nonroutine searches requiring reasonable suspicion.¹⁷² *Riley* demands this conclusion. The Court held that “when privacy-related concerns are weighty enough a search may require a warrant, notwithstanding the diminished expectations of privacy.”¹⁷³

The Fourth and Ninth Circuits have correctly recognized that forensic searches of electronic devices implicate privacy interests far exceeding those of traditional border searches.¹⁷⁴ These searches should require, at minimum, reasonable suspicion that evidence of border-related crimes will be found on

166. *See id.* at 1258.

167. *United States v. Montoya de Hernandez*, 473 U.S. 531, 537, 537–38, 544 (1985).

168. *See United States v. Kolsuz*, 890 F.3d 133, 137 (4th Cir. 2018).

169. *See* 31 U.S.C. § 5317.

170. *See United States v. Hernandez-Salazar*, 813 F.2d 1126, 1133 (11th Cir. 1987).

172. *See id.* at 1138.

172. *See United States v. Cano*, 934 F.3d 1002, 1016 (9th Cir. 2019).

173. *Riley v. California*, 573 U.S. 373, 392 (2014).

174. *United States v. Kolsuz*, 890 F.3d 133, 145, 146 (4th Cir. 2018); *Cano*, 934 F.3d at 1015, 1016; *United States v. Aigbekaen*, 943 F.3d 713, 720 (4th Cir. 2019).

the device.¹⁷⁵ This suspicion must be particularized to each circumstance, not merely a generic assertion that cell phones are used in crimes.¹⁷⁶

The Ninth Circuit's additional requirement that searches be limited to contraband detection provides an important safeguard.¹⁷⁷ The border search exception "authorizes warrantless searches only to determine whether phone contains contraband," not to conduct fishing expeditions for evidence of unrelated domestic crimes.¹⁷⁸

Reasonable suspicion must include the articulable suspicion that the person's electronic device possesses contraband or some evidence sought.

C. *The Warrant Requirement as the Better Rule*

The soundest approach requires warrants for forensic device searches of outbound travelers, subject only to genuine exigent circumstances.¹⁷⁹ This rule best comports with *Riley's* recognition that cell phones implicate qualitatively different privacy interests requiring judicial oversight.¹⁸⁰

Modern technology enables swift warrant applications, undercutting any law enforcement necessity argument.¹⁸¹ As *Riley* emphasized, the ability to obtain a warrant quickly has grown with the advancement of technologies.¹⁸² Requiring warrants imposes no significant burden on legitimate law enforcement while providing crucial protection against abuse.¹⁸³

A warrant requirement also addresses the investigative purpose problem. A neutral magistrate judge can assess whether reasonable suspicion exists and whether the proposed search serves legitimate border-related interests or merely provides a pretext for circumventing normal Fourth Amendment requirements.¹⁸⁴ The magistrate judge serves as a check against the "competitive enterprise of ferreting out crime" unconstrained by constitutional limits.¹⁸⁵

175. *Aigbekaen*, 943 F.3d at 719, 720.

176. *See* *United States v. Gumbs*, 799 F. Supp. 3d 1252, 1259 (S.D. Fla. 2025).

177. *See Cano*, 934 F.3d at 1018, 1019.

178. *Id.* at 1018.

179. *See* *United States v. Smith*, 673 F. Supp. 3d 381, 391 (S.D.N.Y. 2023); *United States v. Sultanov*, 742 F. Supp. 3d 258, 292 (E.D.N.Y. 2024).

180. *Riley v. California*, 573 U.S. 373, 393–94 (2014).

181. *See id.* at 401.

182. *See id.*

183. *See id.* at 401, 403.

184. *See id.* at 382; *Katz v. United States*, 389 U.S. 347, 354 (1967).

185. *See Riley*, 573 U.S. at 382; *Katz*, 389 U.S. at 357.

D. *First Amendment Considerations*

Electronic device searches implicate not only Fourth Amendment privacy rights but also First Amendment interests in speech, association, and press freedom.¹⁸⁶ Contact lists reveal associations; text messages and emails contain expressive content; browsing history shows political and religious affiliations.¹⁸⁷ If the government is trying to prove a conspiracy among various targets, proving an association is the first step. For journalists, lawyers, and others, cell phones contain confidential work product and source information.¹⁸⁸

The First Amendment requires “scrupulous exactitude” when searches burden expressive activity.¹⁸⁹ In *Stanford v. Texas*,¹⁹⁰ the Supreme Court held that nothing less than a warrant could safeguard First Amendment freedoms when searches targeted books and papers.¹⁹¹ The Fourth Amendment grew from the conflict between the Crown and the press over general warrants targeting seditious libel.¹⁹²

Modern cell phones are the digital equivalent of all the books, papers, and correspondence that concerned the Founders.¹⁹³ Permitting suspicionless forensic searches of these devices at the border creates a severe chill on international travel and expressive association.¹⁹⁴ The warrant requirement provides necessary protection for these intertwined constitutional rights.¹⁹⁵

IX. CONCLUSION

The border search exception cannot bear the weight the Fourth Amendment placed upon it in the digital age. Extending this exception to forensic searches of outbound travelers’ electronic devices untethers it entirely from its historical and constitutional justifications. Three principles should guide courts addressing these searches.

First, the border search exception should not apply to outbound travelers whose devices are seized for investigative purposes unrelated to border security. The traditional justifications of sovereignty, contraband

186. See *Stanford v. Texas*, 379 U.S. 476, 485, 486 (1965).

187. See *Riley*, 573 U.S. at 379, 395, 396.

188. See *United States v. Gumbs*, 799 F. Supp. 3d 1252, 1254, 1259 (S.D. Fla. 2025).

189. *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978).

190. 379 U.S. 476 (1965).

191. *Id.* at 485, 486.

192. *Id.* at 482.

193. See *Riley*, 573 U.S. at 393, 394.

194. See *United States v. Cotterman*, 709 F.3d 952, 965, 967 (9th Cir. 2013).

195. See *Stanford*, 379 U.S. at 485.

interdiction, and immigration enforcement focus exclusively on incoming threats; departing travelers present no such concerns.

Second, if any border search authority extends to electronic devices, forensic searches should minimally require reasonable suspicion, specifically related to digital contraband or border-related crimes. *Riley* and *Carpenter* establish that digital information receives heightened Fourth Amendment protection based on its quantity, quality, and intimacy. Courts cannot ignore these principles simply because a search occurs at the border or its functional equivalent.

Third, and preferably, courts should require warrants for forensic device searches of outbound travelers, subject only to exigent circumstances. This rule best protects the privacy and associational rights that modern devices implicate while imposing minimal burden on legitimate law enforcement. A magistrate judge can make this determination.

Will the Supreme Court clarify whether the investigative technique of seizing and searching electronic equipment of outbound travelers not related to the border meets the exception? Or will there be an exception to the border exception? There should be no scenario in the United States where outbound international travelers must surrender their electronic homes of data to the government for review without a warrant.

This allowance would conflict fundamentally with the Fourth Amendment, “a provision of the Constitution which sought to guard against an abuse that more than any one single factor gave rise to American independence.”¹⁹⁶ The digital age demands a constitutional reset.

196. *Harris v. United States*, 331 U.S. 145, 159 (1947) (Frankfurter, J., dissenting); see *Cotterman*, 709 F.3d at 967.