

Maryland Law Review


Volume 78 | Issue 3

Article 5

Cell Phones and the Border Search Exception: Circuits Split over the Line Between Sovereignty and Privacy

Gina R. Bohannon

Follow this and additional works at: <https://digitalcommons.law.umaryland.edu/mlr>

 Part of the [Fourth Amendment Commons](#), [Immigration Law Commons](#), and the [Privacy Law Commons](#)

Recommended Citation

78 Md. L. Rev. 635 (2019)

This Notes & Comments is brought to you for free and open access by the Academic Journals at DigitalCommons@UM Carey Law. It has been accepted for inclusion in Maryland Law Review by an authorized editor of DigitalCommons@UM Carey Law. For more information, please contact smccarty@law.umaryland.edu.

Comment

CELL PHONES AND THE BORDER SEARCH EXCEPTION: CIRCUITS SPLIT OVER THE LINE BETWEEN SOVEREIGNTY AND PRIVACY

GINA R. BOHANNON*

Traditionally, the United States government has had plenary authority to conduct warrantless searches at the international border, and its functional equivalent.¹ The border search exception allows U.S. Customs and Border Protection (“CBP”) and other Department of Homeland Security (“DHS”) personnel to search persons and property entering or exiting the country without obtaining a warrant or, in most cases, articulating any particularized suspicion for the search.² At a growing rate, in addition to x-raying luggage, opening vehicle trunks, and sifting through other containers, CBP personnel have collected cell phones, laptops, and other electronic devices carried across the border and manually examined or downloaded and forensically searched their digital contents.³

In light of growing privacy concerns and the United States Supreme Court’s recent limitations on cell phone searches under other traditional warrant exceptions,⁴ some travelers have argued that the warrantless search of their cell phones, though conducted upon entering or exiting the country, violates the Fourth Amendment.⁵ With no direct ruling from the Supreme

© 2019 Gina R. Bohannon.

* J.D. Candidate, 2020, University of Maryland Francis King Carey School of Law. The author thanks the staff of the *Maryland Law Review* for their tireless efforts, thoughtful feedback, and careful editing and Professor Lee Kovarsky for his valuable guidance. The author also thanks her family for their love and encouragement, especially her husband, Addison Bohannon, for his unwavering support, patience, and insightful conversation.

1. *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004) (quoting *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985)).

2. *Id.* at 152 (quoting *Montoya de Hernandez*, 473 U.S. at 538) (“Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant . . .”).

3. *CBP Releases Statistics on Electronic Device Searches*, U.S. CUSTOMS & BORDER PROTECTION (Apr. 11, 2017), <https://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0> [hereinafter *CBP Releases Statistics*].

4. See *infra* note 26 and accompanying text.

5. See *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (holding the government cannot obtain cell site location information from a third party without a warrant supported by probable

Court, the federal circuit courts have come to diverging conclusions about whether the contours of the border search exception include any or all cell phone searches.⁶

Part I of this Comment will discuss how the Supreme Court recently limited the scope of traditional warrantless investigations, including the third-party doctrine and the search incident to arrest exception, when applied to cell phone records and data.⁷ Part I will also discuss the Court's recognition and development of the border search exception, DHS's interpretation of their authority to search electronic devices under the border search exception, and legislative proposals to limit that authority.⁸ Finally, Part I will describe the circuit split over the question of what, if any, level of individual suspicion is required by the Fourth Amendment for the government to conduct a search of a cell phone at the international border.⁹

Part II of this Comment will argue that cell phone searches should be considered beyond the scope of the border search exception because of heightened individual privacy interests in cell phones and the diminished government interest in the search of digital content at the border.¹⁰ Part II will also question whether creating different standards for manual and forensic searches of cell phones and other electronic devices reflects a meaningful distinction based on the intrusiveness of the search and provides a workable rule for technology that is continuously evolving.¹¹ Finally, Part II will conclude that establishing a warrant requirement for electronic device searches at the border would adequately protect individual privacy interests and reflect the Supreme Court's precedent.¹²

I. BACKGROUND

Customs officers have traditionally conducted routine searches of items entering the United States absent a warrant or probable cause without contravening the Fourth Amendment.¹³ Today, judges and policymakers are re-assessing the balance between the legitimate interests of the government at the border in conducting warrantless investigations and the privacy interests at stake in discretionary searches of cell phones and other personal electronic

cause); *Riley v. California*, 134 S. Ct. 2473 (2014) (holding the government cannot search a cell phone incident to arrest without a warrant supported by probable cause); *see infra* Section I.C.

6. *See infra* Section I.C.

7. *See infra* Section I.A.

8. *See infra* Section I.B.

9. *See infra* Section I.C.

10. *See infra* Section II.A.

11. *See infra* Section II.B.

12. *See infra* Section II.C.

13. *See infra* Section I.B.1.

devices.¹⁴ This Part first discusses how the Supreme Court has recently applied traditional Fourth Amendment principles to obtaining cell phone data in *Carpenter v. United States*¹⁵ and *Riley v. California*.¹⁶ Next, this Part discusses Supreme Court precedents, current executive policies, and proposed legislation governing the border exception and searches of electronic devices.¹⁷ Finally, this Part describes the current circuit split over the question of what, if any, level of individualized suspicion is required for a border search of a cell phone.¹⁸

A. *Digital Searches in the Fourth Amendment Framework*

Since the earliest calls for revolution against British rule, Americans have called for limitations on the government's ability to conduct broad searches of private property.¹⁹ The Fourth Amendment states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.²⁰

The drafters of the Fourth Amendment were immediately concerned with preventing the government from adopting the British practice of issuing general warrants or writs of assistance that allowed officers to conduct searches, unlimited in time or scope, of private property.²¹ As federal regulation and investigative techniques have evolved over time, the Fourth Amendment continues to regulate the extent to which government intrusion into the privacies of individuals' lives is permissible.²²

14. See *infra* Section I.B–C.

15. 138 S. Ct. 2206 (2018).

16. 134 S. Ct. 2473 (2014); see *infra* Section I.A.

17. See *infra* Section I.B.

18. See *infra* Section I.C.

19. In colonial Massachusetts, James Otis challenged the legality of the use of general warrants issued by the British crown against colonists who expressed criticism of the King in a lengthy oration, which John Adams later described as a rallying cry against British rule. See *Riley v. California*, 134 S. Ct. 2473, 2494 (2014) (“Every man of a crowded audience appeared to me to go away, as I did, ready to take arms against writs of assistance. . . . Then and there the child Independence was born.” (quoting 10 THE WORKS OF JOHN ADAMS 247–48 (Charles F. Adams ed., Boston, Little, Brown & Co. 1856))); MASS. HISTORICAL SOCIETY, *Legal Papers of John Adams, volume 2, ADAMS PAPERS DIGITAL EDITION* (2018), <http://www.masshist.org/publications/adams-papers/view?id=ADMS-05-02-02-0006-0002-0001#LJA02d034n1>.

20. U.S. CONST. amend. IV.

21. *Riley*, 134 S. Ct. at 2494.

22. *E.g.*, *United States v. Jones*, 565 U.S. 400 (2012) (determining whether attaching GPS-enabled tracking devices to a suspect's vehicle violates the Fourth Amendment); *Kyllo v. United States*, 533 U.S. 27 (2001) (determining whether the use of a thermal imaging device to monitor

Courts use a two-part inquiry to determine whether the government conducted an unconstitutional search.²³ First, as a threshold matter, the court determines if the government's actions constituted a search, or an intrusion of an individual's "reasonable expectation of privacy," triggering the protections of the Fourth Amendment.²⁴ If so, the court evaluates whether the search was reasonable.²⁵ Generally, a search that is executed in accordance with a valid warrant supported by probable cause is presumed reasonable.²⁶ However, some searches may be reasonable without a warrant if they are conducted pursuant to an established, well-delineated exception to the warrant requirement.²⁷ Searches conducted pursuant to a valid warrant exception are reasonable under the Fourth Amendment when "the nature and quality of the intrusion on the individual's Fourth Amendment interests" are balanced "against the importance of the governmental interests alleged to justify the intrusion."²⁸

The ubiquitous use of electronic devices to store and communicate information has raised questions over how to apply traditional Fourth Amendment doctrines developed for the physical world to digital content.²⁹ The drafters of the Constitution and the Bill of Rights likely could not have imagined the scope of technological advances that today make information about personal lives so easily compressed, transported, copied, and searched. Even just ten years ago, lawmakers and judges perhaps did not contemplate the excessive amounts of personal data now found in small rectangular devices most Americans carry with them at all hours of the day and nearly half

radiation of heat from a person's home violates the Fourth Amendment); *Skinner v. Ry. Labor Excs.' Ass'n*, 489 U.S. 602 (1989) (determining whether a mandatory drug screening program for railroad workers involved in accidents violates the Fourth Amendment); *United States v. Place*, 462 U.S. 696 (1983) (determining whether allowing a drug detection dog to sniff the outside of a bag violates the Fourth Amendment). *See generally* DAVID GRAY, *THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE* 23–55 (2017) (describing modern technologies and expanding governmental surveillance programs that raise Fourth Amendment concerns).

23. *See, e.g.*, *Carpenter v. United States*, 138 S. Ct. 2206, 2221 (2018) (initially determining the acquisition of cell site location information ("CSLI") was a search and subsequently determining the search was not reasonable and thus violated the Fourth Amendment).

24. *Id.* at 2217 (citing *Katz v. United States*, 389 U.S. 347 (1967)).

25. *Id.* at 2221.

26. *Id.* at 2213 (citing *Smith v. Maryland*, 442 U.S. 735, 740 (1979)).

27. *E.g.*, *Brigham City v. Stuart*, 547 U.S. 398 (2006) (exigent circumstances); *Horton v. California*, 496 U.S. 128 (1990) (plain view exception); *United States v. Ramsey*, 431 U.S. 606 (1977) (border exception); *Chimel v. California*, 395 U.S. 752 (1969) (search incident to lawful arrest).

28. *O'Connor v. Ortega*, 480 U.S. 709, 719 (1987) (quoting *United States v. Place*, 462 U.S. 696, 703 (1983)).

29. *See generally* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 533 (2005) (discussing challenges in applying current law to searches and seizures of digital content).

of all Americans say they could not live without.³⁰ Recently, in *Carpenter v. United States* and *Riley v. California* the Supreme Court addressed how the proliferation of smartphones informs the analysis of what constitutes a Fourth Amendment search and whether a search is reasonable.³¹

1. *The Third-Party Doctrine—Carpenter v. United States*

In *Carpenter v. United States*, the Court addressed how cell site location information (“CSLI”), detailed records of a cell phone’s location held by a service provider,³² impacts the third-party doctrine.³³ Traditionally, under the third-party doctrine, the government can secure records and data from third parties without a warrant based on the maxim that “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”³⁴ *Carpenter*, however, sought to suppress cell phone records the FBI obtained from MetroPCS and Sprint without a warrant, which placed his cell phone at the scene of multiple robberies, arguing that these records were beyond the scope of the third-party doctrine.³⁵

The Court agreed with *Carpenter* and distinguished CSLI from other “business records.”³⁶ The Court determined that CSLI is not consistent with the diminished expectation of privacy that underscores the third-party doctrine because it provides “detailed, encyclopedic, and effortlessly compiled” information, giving the government “an intimate window into a person’s life, revealing not only his particular movements, but through them his ‘familial, political, professional, religious, and sexual associations.’”³⁷ The Court held

30. Andrew Perrin, *10 Facts About Cell Phones as the iPhone Turns 10*, PEW RES. CTR. (June 28, 2017), <http://www.pewresearch.org/fact-tank/2017/06/28/10-facts-about-smartphones/>. Seventy-seven percent of adults in the United States own smartphones. *Id.* Of the number of people who own a smartphone, forty-six percent say they could not live without it. *Id.* Smartphones are on track to reach market saturation in a record-setting ten years. Michael DeGusta, *Are Smart Phones Spreading Faster Than Any Technology in Human History?*, MIT TECH. REV. (May 9, 2012), <https://www.technologyreview.com/s/427787/are-smart-phones-spreading-faster-than-any-technology-in-human-history/>.

31. *Carpenter*, 138 S. Ct. at 2216; *Riley v. California*, 134 S. Ct. 2473, 2484 (2014).

32. CSLI creates a record of where a cellular device is located whenever it is turned on and connected to a cellular network based on signals transmitted between a device and a cellular tower. Depending on the density of cell towers, this information can be as precise as or even more accurate than GPS information and can essentially “reconstruct someone’s specific movements down to the minute, not only around town but also within a particular building.” GRAY, *supra* note 22, at 26–27 (quoting *Riley*, 134 S. Ct. at 2490).

33. *Carpenter*, 138 S. Ct. at 2211.

34. *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979).

35. *Carpenter*, 138 S. Ct. at 2212–13.

36. *Id.* at 2219–20.

37. *Id.* at 2216, 2217 (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

that although CSLI was discoverable, it could not be obtained without a warrant supported by probable cause.³⁸

2. *The Search Incident to Arrest Exception—Riley v. California*

Under the search incident to arrest doctrine, no warrant or probable cause is required for law enforcement officers to search persons being arrested and anything within the arrestee's area of immediate control.³⁹ This type of search has traditionally been justified by the government's interest in ensuring law enforcement officers' safety and preventing the destruction of evidence.⁴⁰ The search incident to arrest doctrine has been used expansively to support the search of even innocuous-seeming possessions of an arrestee, including the contents of a crumpled cigarette box.⁴¹ However, in *Riley v. California*, the Supreme Court limited this doctrine from permitting the search of a cell phone without a warrant.⁴²

After being pulled over for an expired license plate, Riley was eventually arrested for possession of concealed and loaded firearms discovered when his car was impounded and inventoried.⁴³ Incident to his arrest, police seized a cell phone from Riley's pants pocket and examined the contents, discovering text messages, pictures, and videos that indicated he was involved with the "Bloods" street gang and connected him to a recent shooting.⁴⁴ In a companion case, *United States v. Wurie*,⁴⁵ officers seized a "flip phone"⁴⁶ from Wurie after he was arrested for selling drugs on the street.⁴⁷ Officers used the call history and photographs on the phone to locate an apartment, at which, after obtaining a search warrant, officers discovered more drugs and other evidence of significant drug trafficking.⁴⁸ Riley and Wurie

38. *Id.* at 2221.

39. *Chimel v. California*, 395 U.S. 752, 763 (1969).

40. *Riley v. California*, 134 S. Ct. 2473, 2483–85 (2014) (citing *Chimel*, 395 U.S. at 753–54).

41. *United States v. Robinson*, 414 U.S. 218, 236 (1973).

42. *Riley*, 134 S. Ct. at 2485.

43. *Id.* at 2480. The search of Riley's vehicle which led to the discovery of the firearms was not supported by a warrant or any particular suspicion. *Id.* It was justified by a recognized warrant exception for inventory searches. *Id.*; see *Harris v. United States*, 390 U.S. 234, 236 (1968) (per curiam) (upholding the search of arrestee's impounded vehicle).

44. *Riley*, 134 S. Ct. at 2480–81.

45. *United States v. Wurie*, 728 F.3d 1 (1st Cir. 2013), *aff'd sub nom.* *Riley v. California*, 134 S. Ct. 2473 (2014).

46. Flip phones, a common type of mobile phone that is flipped open for use, popular before the development of smartphones, have fewer capabilities and store less data than a smartphone. *Riley*, 134 S. Ct. at 2481. Flip phones can store, among other data, photos, contact lists, and call history. *Id.*

47. *Id.*

48. *Id.*

argued that the searches of their cell phones without a warrant violated the Fourth Amendment.⁴⁹

The Court agreed, emphasizing that both the quantity and quality of information stored on cell phones significantly increased the privacy interests and expectations of individuals carrying them.⁵⁰ The Court also remarked on the pervasiveness of cell phone use in terms of both the percentage of people using the devices regularly and the manner in which they are used to monitor and record nearly every aspect of a person's day-to-day life.⁵¹

In addition to finding that the individual privacy interests at stake in cell phone searches were higher than in searches of physical items, the Court also remarked that cell phone searches are not justified by the government concerns that underlie the search incident to arrest exception⁵²: Cell phone data poses no threat to the safety of officers and is not at risk of being destroyed as evidence once in the possession of law enforcement.⁵³

The Court rejected other rules proffered by the government to curtail arrestee cell phone searches without prohibiting them altogether.⁵⁴ One of the Court's concerns was how to distinguish between data stored on the actual device the individual was carrying and data readily retrieved from remote data centers.⁵⁵ The government conceded that the search incident to arrest exception could not be stretched to search files stored on the cloud, since, in the Court's analogy, that would be tantamount to finding a key on the individual and being permitted to search the entire contents of his house.⁵⁶ The Court also rejected the idea that police could search cell phone data that had a physical analog for two reasons.⁵⁷ First, though the content may be equivalent, it would be unlikely or impossible for an individual to carry all the

49. *Id.* at 2481–82.

50. *Id.* at 2489.

51. *Id.* at 2490 (“[T]he phrase ‘there’s an app for that’ is now part of the popular lexicon.”).

52. *Id.* at 2485–87.

53. *Id.* The Court found the argument that officers could intercept important communications for co-conspirators to prevent future harm did not justify the warrantless search. *Id.* at 2486. These types of circumstances, the Court reasoned, could better be dealt with under the doctrine of exigent circumstances. *Id.* The Court also was not persuaded by the government's concerns about remote data wiping of devices and data encryption. *Id.* at 2486–87.

54. *Id.* at 2491.

55. *Id.*

56. *Id.* This distinction highlights another tension between doctrines for physical searches and the digital world. For more discussion on the location-driven approach to digital information, see Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 186–91 (2018).

57. *Riley*, 134 S. Ct. at 2493.

digital content on their cell phone in physical form.⁵⁸ Second, the Court believed this rule would be too difficult for law enforcement officers and courts to apply.⁵⁹

B. The Border Search Exception

Like the third-party doctrine and the search incident to arrest exception, the border search exception is a historically recognized Fourth Amendment doctrine that allows the government to conduct an investigation without obtaining a warrant.⁶⁰ A border search is a search of a person or property upon entering or departing the country.⁶¹ Border searches occur at the actual geographic boundary and at other points of entry, including international airports.⁶² The Court's protective treatment of cell phone data under other traditional warrant exceptions prompts questions about whether the border search exception should also be limited when applied to personal electronic devices.⁶³

This Section first describes Supreme Court precedent governing border searches.⁶⁴ Next, this Section discusses current DHS policies on the execution of border searches of electronic devices and proposed legislation that would provide further limitations.⁶⁵

1. Origins and Historical Justification of the Border Search Exception

Historically, border searches have been deemed reasonable without a warrant because of the compelling government interest in controlling who and what may cross into the nation's sovereign territory.⁶⁶ The Constitution gives the federal government various specific powers that require oversight of what persons and property cross the border, including the power to "provide for the common defence,"⁶⁷ "regulate commerce with foreign nations,"⁶⁸

58. *Id.* ("It is implausible that [Riley] would have strolled around with video tapes, photo albums, and an address book all crammed into his pockets.").

59. *Id.*

60. *United States v. Flores-Montano*, 541 U.S. 149, 152–53 (2004) (citing *United States v. Ramsey*, 431 U.S. 606, 616 (1977)).

61. *See United States v. Kolsuz*, 890 F.3d 133, 137–38 (4th Cir. 2018) (citing *United States v. Oriakhi*, 57 F.3d 1290, 1296–97 (4th Cir. 1995)) (explaining that rationales underlying the border search exception extend equally to exit and entry searches).

62. *Id.* at 137.

63. *See infra* Part II.

64. *See infra* Section I.B.1.

65. *See infra* Section I.B.2–3.

66. *United States v. Montoya de Hernandez*, 473 U.S. 531, 537–38 (1985) (citing *United States v. Ramsey*, 431 U.S. 606, 618–19 (1977)).

67. U.S. CONST. art. I, § 8, cl. 1.

68. U.S. CONST. art. I, § 8, cl. 3.

and “establish an uniform rule of naturalization.”⁶⁹ Throughout history, the government has relied on interdiction at the border to meet contemporary challenges to these objectives.⁷⁰

In its fifth act of legislation, the first Congress of the United States passed a law establishing the United States Customs Service on July 31, 1789.⁷¹ The Customs Service was responsible for collecting tariffs on imported goods critical to financing the new government at ports of entry on the international border.⁷² The law enabled customs officers “to open and examine” the items transported across the border and gave officers the “full power and authority, to enter any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed; and therein to search for, seize, and secure any such goods.”⁷³ While the law instructed customs officers to apply for a warrant to search a “dwelling-house, store, building, or other place” suspected of concealing goods subject to a duty, no such warrant was required on ships or containers moving across the border.⁷⁴

The Fourth Amendment was officially ratified two years later on December 15, 1791, with the rest of the Bill of Rights.⁷⁵ As was recognized by the Supreme Court in *Boyd v. United States*,⁷⁶ one of the oldest Supreme Court cases to recognize the border search exception, the temporal proximity of these acts shows that those who originally contemplated the Constitution’s prohibition of unreasonable searches recognized the difference in the balance of government and private interests between searches in the interior and at the border.⁷⁷

69. U.S. CONST. art. I, § 8, cl. 4.

70. During the period following the Revolutionary War, the United States relied on customs inspectors to ensure duties were properly paid on goods traded with other countries, which was important for establishing the United States in the interstate economy and raising revenue to pay the nation’s debts. See *Boyd v. United States*, 116 U.S. 616, 623 (1886) (discussing early customs revenue laws of the United States). The government has also used border checkpoints to prevent contraband from entering the United States during the Prohibition era and later during the War on Drugs. See *Montoya de Hernandez*, 473 U.S. at 538 (discussing the role border searches may play in protecting the nation from “the veritable national crisis in law enforcement caused by smuggling of illicit narcotics”).

71. Act of Jul. 31, 1789, Sess. I, ch. 5.

72. *Id.* § 22.

73. *Id.* §§ 23–24.

74. *Id.* § 24.

75. U.S. CONST. amend. I–X.

76. 116 U.S. 616 (1886).

77. *Id.* at 623; see *United States v. Ramsey*, 431 U.S. 606, 616–17 (1977) (“As this act was passed by the same Congress which proposed for adoption the original amendments to the Constitution, it 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.” (quoting *Boyd v. United States*, 116 U.S. 616, 623 (1886))).

The distinction between searches at the border and inside the United States was emphasized by the Supreme Court in *Carroll v. United States*.⁷⁸ The Court stated that although it would be unreasonable for prohibition agents to stop every car lawfully using the highways “on the chance of finding liquor,” all travelers could be stopped when “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.”⁷⁹

Six years after President Nixon officially declared a “War on Drugs,”⁸⁰ the Supreme Court affirmed the importance and permissibility of warrantless border searches in *United States v. Ramsey*.⁸¹ The Court upheld the opening of mailed envelopes that were suspected of containing illegal drugs, without a warrant or probable cause, denying any difference between packages that were mailed and those that were carried by an individual across the border.⁸² “It is their entry into this country from without it that makes a resulting search ‘reasonable.’”⁸³ The Court also emphasized that the “historically recognized” border search exception is not based on the doctrine of exigent circumstances “at all,” but rather is a historical doctrine of independent justification similar to the “search incident to lawful arrest” exception.⁸⁴ Still, the Court noted that although most border searches were presumptively reasonable without a warrant, a border search might be deemed “unreasonable” due to “the particularly offensive manner in which it is carried out,” but declined to opine under what circumstances.⁸⁵

2. Distinguishing Routine and Nonroutine Border Searches

Eight years later, in *United States v. Montoya de Hernandez*,⁸⁶ the Court identified a search that was, as alluded to in *Ramsey*, conducted in such an offensive and intrusive manner that, unlike other routine border searches, it

78. 267 U.S. 132 (1925).

79. *Id.* at 154.

80. At a press conference on June 17, 1971, President Nixon called drug abuse “public enemy number one.” Chris Barber, *Public Enemy Number One: A Pragmatic Approach to America’s Drug Problem*, RICHARD NIXON FOUND. (June 29, 2016), <https://www.nixonfoundation.org/2016/06/26404/>. Nixon described multi-faceted policy approach to “wage a new, all-out offensive” to “fight and defeat this enemy” which included increasing enforcement abroad and within the United States. *Id.*

81. 431 U.S. 606, 616 (1977).

82. *Id.* at 620.

83. *Id.*

84. *Id.* at 621.

85. *Id.* at 618 n.13.

86. 473 U.S. 531 (1985).

was unconstitutional without individualized suspicion.⁸⁷ Montoya de Hernandez arrived at the Los Angeles International Airport on a flight from Bogotá, Colombia.⁸⁸ After questioning Montoya de Hernandez and conducting a pat down and strip search, customs agents suspected that she was smuggling drugs in her alimentary canal.⁸⁹ Refusing to submit to an x-ray inspection, Montoya de Hernandez was detained in a customs office for observation until she produced a bowel movement.⁹⁰ After several hours passed, customs officials obtained a court order authorizing a rectal examination and involuntary x-ray.⁹¹ A physician removed a balloon filled with cocaine from Montoya de Hernandez's body and Montoya de Hernandez was arrested.⁹²

The Court held that detention at the international border beyond "a routine customs search and inspection" is only permissible if customs agents "reasonably suspect that the traveler is smuggling contraband in her alimentary canal."⁹³ The Court explained that in Montoya de Hernandez's case, the reasonable suspicion standard appropriately balanced the "private and public interests" at stake.⁹⁴ Justice Brennan wrote a strong dissent joined by Justice Marshall arguing that even at the international border, the detention of Montoya de Hernandez and other investigations that involved highly intrusive techniques, such as body-cavity searches, x-rays, and stomach-pumping, are barred by the Fourth Amendment without a warrant.⁹⁵

The Court declined to extend the reasonable suspicion requirement to a border search of a vehicle in *United States v. Flores-Montano*⁹⁶ in which the

87. See *Ramsey*, 431 U.S. at 618 n.13 (discussing the possibility that a border search could at some point become "unreasonable").

88. *Montoya de Hernandez*, 473 U.S. at 533.

89. *Id.* Their suspicion was based on answers to questioning about her travel plans, recent travel history, the "firm fullness" of her abdomen, and multiple pairs of underpants discovered during the strip search. *Id.* at 533–34.

90. *Id.* at 534–35.

91. *Id.* at 535. At this point, Montoya de Hernandez had been in custody for almost twenty-four hours. *Id.*

92. *Id.* Over the next four days she passed eighty-eight balloons filled with a total of 528 grams of eight percent pure cocaine hydrochloride. *Id.* at 536.

93. *Id.* at 541.

94. *Id.* The government interest was high considering not only the "longstanding concern for the protection of the integrity of the border," but also the "veritable national crisis in law enforcement caused by smuggling of illicit narcotics." *Id.* at 538. Additionally, the Court recognized that an alimentary canal smuggler generally "gives no external signs" and would rarely give rise to a probable cause standard. *Id.* at 541. Although the Court did not articulate specifically what aspects of the search made it "beyond the scope of a routine customs search," the length of time of the detention and humiliation suffered by Montoya de Hernandez while being monitored for a bowel movement made the search distinctly offensive. *Id.* Ultimately, the search was deemed lawful because the Court determined that customs officers had the requisite reasonable suspicion at the time of the search. *Id.* at 542.

95. *Id.* at 551–52 (Brennan, J., dissenting).

96. 541 U.S. 149, 152 (2004).

vehicle's gas tank was completely disassembled by customs officers.⁹⁷ The Court upheld the search, which yielded illicit drugs, denying that the vehicle owner had any privacy interest in his gas tank.⁹⁸ The Court also found that no damage was done to the fuel tank or vehicle during the search, and, therefore, declined to opine on whether or to what extent property may be damaged in a suspicionless border search.⁹⁹

Aside from the alimentary canal search in *Montoya de Hernandez*, the Supreme Court has never required any particularized suspicion to justify a search at the border.¹⁰⁰ However, several federal courts of appeals have required a reasonable suspicion standard for other searches deemed "nonroutine."¹⁰¹ These types of searches include strip searches,¹⁰² x-ray searches,¹⁰³ searches requiring the removal of an artificial limb,¹⁰⁴ the drilling of permanent holes into property,¹⁰⁵ and an extensive search of a laptop computer.¹⁰⁶

3. *Current Homeland Security Policies and Proposed Legislation*

While customs inspections at the border are still critical for collecting duties and facilitating international trade, today CBP also conducts operations focused on combating international drug trafficking, terrorism, and illegal immigration.¹⁰⁷ According to CBP, the agency apprehends more than 1100 individuals for suspected crimes and seizes nearly four tons of illicit drugs a day.¹⁰⁸

97. *Id.* at 151.

98. *Id.* at 154.

99. *Id.* The Court did not affirm or deny the reasoning of the multiple circuit courts that required reasonable suspicion to drill holes, causing permanent damage, to vehicles or other containers crossing the border. *Id.* at 154 n.2. The Court also "[le]ft open the question 'whether, and under what circumstances, a border search [of property] might be deemed 'unreasonable.'" *Id.* (quoting *United States v. Ramsey*, 431 U.S. 606, 618 n.13 (1977)).

100. *United States v. Touset*, 890 F.3d 1227, 1233 (11th Cir. 2018). *But see Ramsey*, 431 U.S. at 625 (Powell, J., concurring) (discussing the importance of the effect of federal statutes which required "reasonable cause to suspect" contraband was present to conduct a search in protecting individual Fourth Amendment rights (citing 19 U.S.C. § 482)).

101. *See supra* notes 102–106 and accompanying text.

102. *United States v. Uricoechea-Casallas*, 946 F.2d 162, 166 (1st Cir. 1991).

103. *United States v. Vega-Bravo*, 729 F.2d 1341, 1349 (11th Cir. 1984).

104. *United States v. Sanders*, 663 F.2d 1, 3 (2d Cir. 1981).

105. *United States v. Rivas*, 157 F.3d 364, 367 (5th Cir. 1998); *United States v. Robles*, 45 F.3d 1, 5 (1st Cir. 1995); *United States v. Carreon*, 872 F.2d 1436, 1442 (10th Cir. 1989).

106. *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) (en banc).

107. *See About CBP*, U.S. CUSTOMS & BORDER PROTECTION, <https://www.cbp.gov/about> (last modified Nov. 21, 2016) (explaining that CBP "is charged with keeping terrorists and their weapons out of the U.S." in addition to "facilitating lawful international travel and trade"). CBP's mission is to "safeguard America's borders thereby protecting the public from dangerous people and materials while enhancing the Nation's global economic competitiveness by enabling legitimate trade and travel." *Id.*

108. *Id.*

In recent years, CBP has increased its execution of cell phone and computer searches.¹⁰⁹ During the first six months of fiscal year 2017, CBP searched the electronic devices of 14,993 travelers coming into the United States.¹¹⁰ Although this only represents a very small fraction of arriving individuals, it is a rate that is four times higher than it was in 2015.¹¹¹ CBP defends its increased use of digital searches as necessary to meet their “mission to protect the American people and enforce the nation’s laws in this digital age.”¹¹² Border searches of electronic devices have resulted in evidence to “combat[] terrorist activity, child pornography, violations of export controls, intellectual property rights violations, and visa fraud.”¹¹³

In 2018, U.S. Congressional Representatives and Senators proposed legislation “to place restrictions on searches and seizures of electronic devices at the border”¹¹⁴ that proscribes standards for how DHS personnel should conduct inspections of electronic devices entering or exiting the country to balance the important government and private interests at stake.

a. Current DHS Electronic Device Search Policies

In January 2018, CBP updated their official policy on how and when officers should inspect electronic devices at the border.¹¹⁵ According to the policy, the extent of the search may be limited based on whether it is defined as a “basic search” or an “advanced search.”¹¹⁶ An advanced search is defined by CBP as “any search in which an Officer connects external equipment . . . to an electronic device . . . to review, copy, and/or analyze its contents.”¹¹⁷ Basic searches are defined as those that are “not an advanced search.”¹¹⁸

109. *CBP Releases Statistics*, *supra* note 3; *see also* Kaveh Waddell, *The Steady Rise of Digital Border Searches*, ATLANTIC (Apr. 12, 2017), <https://www.theatlantic.com/technology/archive/2017/04/the-steady-rise-of-digital-border-searches/522723/>.

110. This number represents .008% of all arrivals. *CBP Releases Statistics*, *supra* note 3.

111. *Id.*

112. *Id.*

113. *Id.*

114. S. 2462, 115th Cong. (2018).

115. U.S. CUSTOMS AND BORDER PROTECTION, CBP DIRECTIVE NO. 3340-049A, (Jan. 4, 2018), <https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf> [hereinafter CBP DIRECTIVE NO. 3340-049A]. Electronic devices are defined broadly as “[a]ny device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players.” *Id.* ¶ 3.2. This new policy includes significant updates from the previous 2009 policy. *See* U.S. CUSTOMS AND BORDER PROTECTION, CBP DIRECTIVE NO. 3340-049 (Aug. 20, 2009), https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf.

116. CBP DIRECTIVE NO. 3340-049A, *supra* note 115, ¶¶ 5.1.3–4.

117. *Id.* ¶ 5.1.4.

118. *Id.* ¶ 5.1.3.

The policy references case law supporting the proposition that border searches are “not subject to any requirement of reasonable suspicion, probable cause, or warrant.”¹¹⁹ However, though a basic search may be conducted “with or without suspicion,”¹²⁰ the policy states that an advanced search may be performed when there is “reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern.”¹²¹

The policy sanctions physical inspection of an electronic device and examination of information stored on the device itself, but specifically prohibits, in all instances, the intentional access of information stored remotely.¹²² The policy also instructs CBP officers to request assistance from travelers in unlocking passcode-protected or encrypted data.¹²³ If a traveler refuses to unlock the device or the inspection cannot otherwise be completed, the officer may detain the device.¹²⁴

Immigration and Customs Enforcement (“ICE”) has not released an updated electronic device border search policy since August 2009.¹²⁵ Unlike the new CBP policy, the ICE policy does not distinguish between “advanced” and “basic” searches.¹²⁶ The ICE policy maintains that ICE agents “may search, detain, seize, retain, and share electronic devices, or information contained therein, with or without individualized suspicion.”¹²⁷ The policy also does not distinguish between information discovered on the device and information obtained via the device from other remote storage locations.¹²⁸

119. *Id.* ¶ 4 (quoting *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985)).

120. *Id.* ¶ 5.1.3.

121. *Id.* ¶ 5.1.4.

122. *Id.* ¶ 5.1.2. To facilitate this objective, the policy encourages officers to request that the traveler disable network connectivity by placing the device in airplane mode or by other means. *Id.*

123. *Id.* ¶ 5.3.1.

124. *Id.* ¶ 5.3.3. Scholars have questioned whether forcing individuals to give up passwords to unlock protected files contravenes the Fifth Amendment protection against self-incrimination. For discussion of potential Fifth Amendment concerns with this practice see, for example, Lauren Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 *FORDHAM L. REV.* 203 (2018). The CBP policy also states that electronic devices or copies of information gathered from devices may only be retained after an inspection if there is probable cause that it “contains evidence of a violation of law that CBP is authorized to enforce or administer” or is “information relating to immigration, customs, and other enforcement matters.” *CBP DIRECTIVE NO. 3340-049A*, *supra* note 115, ¶¶ 5.5.1.1–.3. All other electronic records will be “destroyed” within seven days of such a determination, and the electronic device will be returned. *Id.* ¶ 5.4.1.2. However, if more time is required by the “circumstances” a supervisor may approve the retention of information up to twenty-one days. *Id.*

125. U.S. IMMIGRATION & CUSTOMS ENFORCEMENT, *DIRECTIVE NO. 7-6.1* (Aug. 18, 2009), https://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf.

126. *Id.*

127. *Id.* ¶ 6.1.

128. *Id.* ¶ 5.1.

b. Proposed Legislation

On February 27, 2018, Senators Patrick Leahy (D-VT) and Steve Daines (R-MT) introduced Senate Bill 2462—“a bill [t]o place restrictions on searches and seizures of electronic devices at the border.”¹²⁹ The bill requires individualized suspicion for all electronic device searches,¹³⁰ and places other limitations on current DHS policies.¹³¹

Senate Bill 2462 distinguishes between “manual” and “forensic” searches of digital devices.¹³² Forensic searches are any searches that take longer than four hours, involve “copying or documentation of data stored on the device,” or are conducted with the assistance of other electronic devices or passwords.¹³³ Manual searches are those conducted without “assistance of any other electronic device, electronic equipment, or software” or “the entry of any password, passcode, fingerprint, account information, or other biometric identifier” that gives access to protected data.¹³⁴

Under the proposed legislation, manual searches would generally only be permitted if a homeland security officer had “reasonable suspicion” that an individual is either carrying contraband or is not legally permitted to enter the United States.¹³⁵ Seizure of electronic devices and “forensic searches” would only be permitted if an officer has probable cause that the person is carrying contraband, not legally admissible to the United States, or violating any law punishable by more than one year “and the electronic device contains information or evidence relevant” to the violation.¹³⁶ Forensic searches would only be permitted after obtaining a warrant by a court of competent jurisdiction.¹³⁷

129. S. 2462, 115th Cong. (2018).

130. During the previous legislative session, a more restrictive bill entitled “The Protecting Data at the Border Act” was introduced in both chambers of Congress. H.R. 1899, 115th Cong. (2017); S. 823, 115th Cong. (2017). The Act would prevent seizing, copying, or retaining any electronic device or information obtained from them without a warrant or probable cause that they contained evidence of a felony. H.R. 1899 § 5(a)(1). The bills were referred to the House Subcommittee on Crime, Terrorism, Homeland Security, and Investigation and the Senate Subcommittee on Federal Spending Oversight Management, but never advanced to the House or Senate floor.

131. S. 2462 § 1(2).

132. *Id.*

133. *Id.* § 1(1).

134. *Id.* § 1.

135. *Id.* § 2(b).

136. *Id.* § 2(c)(2).

137. *Id.* § 2(d). The bill also includes various provisions which require the Department of Homeland Security to record and report several statistics regarding the number of searches and demographics of travelers whose electronic devices were searched, and the number of those searched who were later charged with a criminal offense based on information obtained by the border search. *Id.* § 3.

The bill was referred to the Committee on Homeland Security and Governmental Affairs which held a hearing on the issue on July 11, 2018, but has not been brought to the Senate floor.

C. Border Search Circuit Split

In opinions issued two weeks apart, the United States Court of Appeals for the Fourth and Eleventh Circuits came to conflicting conclusions after considering what, if any, level of suspicion is required for law enforcement officers to conduct forensic searches of digital devices traveling across the international border.¹³⁸ Although courts have contemplated this issue before,¹³⁹ these cases are the first circuit courts of appeals to decide the issue following the Supreme Court's ruling on smartphone searches in *Riley v. California*.¹⁴⁰ The United States Courts of Appeals for the Fifth,¹⁴¹ Seventh,¹⁴² Ninth,¹⁴³ and Tenth¹⁴⁴ Circuits also received direct challenges to cell phone searches at the border in 2018 but have not reached definitive rulings on the question.¹⁴⁵ Lower courts in several circuits have continued to grapple with the question as well.¹⁴⁶

138. *See* *United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018) (holding reasonable suspicion was required to conduct a forensic search of a cell phone at the border); *United States v. Touset*, 890 F.3d 1227, 1230 (11th Cir. 2018) (holding no level of individualized suspicion is required to conduct a forensic search of electronic devices at the border).

139. *See, e.g.,* *United States v. Cotterman*, 709 F.3d 952, 968 (2013) (en banc) (holding a forensic examination of the defendant's computer required a showing of reasonable suspicion).

140. 134 S. Ct. 2473, 2480 (2014).

141. *United States v. Molina-Isadoro*, 884 F.3d 287, 289 (5th Cir. 2018) (choosing not to decide how the border search exception is affected by *Riley* because the non-forensic border search of the defendant's cell phone was supported by probable cause).

142. *United States v. Wanjiku*, No. 16 CR 296, 2017 WL 1304087, at *5 (N.D. Ill. Apr. 6, 2017), *argued*, No. 18-1973 (7th Cir. Nov. 7, 2018).

143. *United States v. Cano*, 222 F. Supp. 3d 876, 882–83 (S.D. Cal. 2016), *appeal docketed*, No. 17-50151 (9th Cir. Apr. 28, 2017).

144. *United States v. Williams*, No. 16-CR-249 (D. Colo.), *appeal docketed*, No. 18-1299 (10th Cir. July 27, 2018).

145. The Court of Appeals for the Fifth Circuit refused to suppress evidence from a warrantless search of an international traveler's cell phone under the good faith exception. *Molina-Isadoro*, 884 F.3d at 289. The court, however, expressly avoided reaching the question of what level of suspicion is required for cell phone searches at the border, instead determining that because CBP agents had probable cause and only conducted a manual search of the defendant's phone, they acted reasonably in light of existing law. *Id.* at 290.

146. *E.g.,* *Alasaad v. Nielsen*, No. 17-cv-11730-DJC, 2018 WL2179323, at *1 (D. Mass. May 9, 2018); *United States v. Caballero*, 178 F. Supp. 3d 1008, 1011 (S.D. Cal. 2016); *United States v. Kim*, 103 F. Supp. 3d 32, 34 (D. D.C. 2015), *appeal dismissed*, No. 15-3035, 2015 WL 5237696 (D.C. Cir. Aug. 14, 2015). The same week that the Eleventh Circuit split from the Fourth Circuit, the United States District Court for the District of Massachusetts denied a motion to dismiss a civil case seeking a declaratory judgment that the current CBP and ICE policies for electronic device searches violate the Fourth Amendment, departing from a previous ruling on a similar challenge decided six years prior. *Alasaad*, 2018 WL2179323, at *14.

1. *The Eleventh Circuit View: No Particularized Suspicion is Required to Search an Electronic Device at the Border*

According to the Court of Appeals for the Eleventh Circuit, only a particularly intrusive search of a person can be considered a nonroutine border search that requires reasonable suspicion;¹⁴⁷ border searches of property, including extensive searches of cell phone data, do not require any level of particularized suspicion.¹⁴⁸ The Eleventh Circuit affirmed this view in two separate cases in 2018, *United States v. Vergara*¹⁴⁹ and *United States v. Touse*.¹⁵⁰

First, in *Vergara*, the Eleventh Circuit held that a forensic search of a cell phone at the border was reasonable without a warrant or probable cause.¹⁵¹ Vergara, a U.S. citizen, was returning to Florida from an international cruise when he was singled out by CBP for additional screening.¹⁵² A lookout notice had been attached to his name based on a previous conviction for possession of child pornography.¹⁵³ CBP agents began manually looking through the pictures and videos on a cell phone in his luggage.¹⁵⁴ After finding a questionable video, a homeland security agent decided to forensically search all three cell phones he was carrying.¹⁵⁵ The searches revealed more than 100 videos and images of child pornography.¹⁵⁶ Vergara was charged with transporting and possessing child pornography.¹⁵⁷ The United States District Court for the Middle District of Florida denied Vergara's motion to suppress the evidence obtained from his cell phone, rejecting his argument that based on the Supreme Court's decision in *Riley v. California*, any search of a cell phone is beyond the reach of the border exception and, therefore, a warrant supported by probable cause is required.¹⁵⁸

In a split decision, the court of appeals affirmed the district court ruling and determined that “[b]order searches ‘never’ require probable cause or a

147. *United States v. Touse*, 890 F.3d 1227, 1231–34 (11th Cir. 2018).

148. *Id.* at 1234.

149. 884 F.3d 1309 (11th Cir. 2018), *cert denied*, 139 S. Ct. 70 (2018).

150. 890 F.3d 1227 (11th Cir. 2018).

151. *Id.*

152. *Id.*

153. *Id.* A lookout is a notice recorded in the TECS System: Primary and Secondary Processing (“TECS”) information sharing platform used by DHS that notifies other users that agents should conduct additional screening of an individual. U.S. DEP’T OF HOMELAND SEC., TECS SYSTEM: PLATFORM 2 (2016), <https://www.dhs.gov/sites/default/files/publications/DHS-PIA-ALL-021%20TECS%20System%20Platform.pdf>.

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

155. *Id.* at 1311 (majority opinion).

156. *Id.*

157. *Id.*

158. *Id.* at 1312.

warrant.”¹⁵⁹ Some “highly intrusive” border searches “of a person’s body such as a strip search or an x-ray examination” require reasonable suspicion, but, the court pointed out, this was a search of property not a person.¹⁶⁰ The court determined that *Riley*’s warrant requirement for cell phones was limited to searches conducted pursuant to a search incident to arrest and did not apply to a border search.¹⁶¹

In dissent, Judge Jill Pryor concluded that a forensic search of a cell phone at the border requires a warrant supported by probable cause.¹⁶² Although Judge Pryor recognized that the Government’s interest at the border is “at its zenith,” she found that the privacy interests in a forensic cell phone search required additional protections.¹⁶³ She noted the Supreme Court’s strong language about the nature of data contained on cell phones in *Riley* and pointed out that “the privacy interests implicated in *forensic* searches are even greater than those involved in the manual searches at issue in *Riley*.”¹⁶⁴ She also reasoned that the purpose of the border exception was to prevent “physical contraband . . . communicable diseases, narcotics, or explosives” from crossing the border, which are not found in cellphone data.¹⁶⁵ In contrast, she questioned whether the government’s electronic border searches are necessary or effective means of intercepting digital evidence since “electronic contraband is borderless” and need not be physically moved through a border checkpoint to enter the country.¹⁶⁶

Two months after issuing their decision in *Vergara*, the Eleventh Circuit affirmed its majority position in *United States v. Touse*t.¹⁶⁷ The court explicitly recognized its disagreement with an intervening opinion issued by the Fourth Circuit¹⁶⁸ and reaffirmed its holding that no level of individualized suspicion is required for a search of electronic devices under the border search exception.¹⁶⁹

Like Vergara, Karl Touse, a U.S. citizen, was returning home from a trip to Mexico when he arrived at the Atlanta International Airport.¹⁷⁰ Prior to his travels, DHS placed a lookout on Touse based on information obtained

159. *Id.* (citing *United States v. Ramsey*, 431 U.S. 606, 619 (1977)).

160. *Id.* (quoting *United States v. Alfaro-Moncada*, 607 F.3d 720, 729 (11th Cir. 2010)).

161. *Id.*

162. *Id.* at 1318–19 (Pryor, J., dissenting).

163. *Id.* at 1314 (quoting *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004)).

164. *Id.* at 1315 (alteration in original).

165. *Id.* at 1317.

166. *Id.*

167. 890 F.3d 1227 (11th Cir. 2018).

168. *See United States v. Kolsuz*, 890 F.3d 127, 146 (4th Cir. 2018) (holding a forensic search of a cell phone is a nonroutine border search that requires at least reasonable suspicion).

169. *Touse*t, 890 F.3d at 1234.

170. *Id.* at 1230.

from a preliminary Cyber Crime Center investigation that suggested he was involved with child pornography and sexual exploitation of children.¹⁷¹ A CBP officer inspecting Touset's luggage obtained his two laptops, two external hard drives, and two tablets.¹⁷² Based largely on DHS's lookout, CBP conducted a forensic analysis of the devices, which took seventeen days and revealed child pornography.¹⁷³ Based on the illicit files obtained from the forensic search of Touset's devices, DHS agents obtained a warrant to search Touset's home, which revealed further evidence that he had purchased child pornography from the Philippines.¹⁷⁴

After being indicted on multiple counts of receiving, transporting and shipping, and possessing child pornography, Touset filed a motion to suppress the evidence obtained from the search of his electronic devices at the border, as well as the fruit of those searches, arguing that CBP did not have the appropriate level of suspicion to lawfully conduct the search.¹⁷⁵ The United States District Court for the District of Georgia denied Touset's motion.¹⁷⁶ Relying on the Ninth Circuit's decision in *United States v. Cotterman*,¹⁷⁷ the court held that reasonable suspicion was required for a forensic border search of an electronic device but found that CBP had reasonable suspicion when they detained and conducted the forensic search of Touset's laptops and hard drives.¹⁷⁸

The court of appeals affirmed the district court's judgment that the evidence should not be suppressed but disagreed with the determination that an elevated level of individualized suspicion was required to conduct a forensic search of an electronic device at the border.¹⁷⁹ The court again stressed that *Riley*'s treatment of cell phone searches does not apply to border searches but is only required to balance the interests at stake in searches incident to an arrest.¹⁸⁰

171. *Id.* Xoom, a money transferring company, identified Touset and other customers it suspected were involved in child pornography based on their history of frequent low money transfers to source countries for sex tourism and child pornography and reported their suspicion to the National Center for Missing and Exploited Children. *Id.* Yahoo also reported tips to the Center based on their own investigation of personal email accounts. *Id.* With this information, the Cyber Crime Center of DHS began its own investigation and was able to link Touset to a suspected supplier of child pornography in the Philippines. *Id.*

172. *Id.*

173. *Id.*

174. *Id.* Nothing in the opinion suggests the child pornography in his possession was obtained during or was related to his recent trip to Mexico.

175. *Id.* at 1231.

176. *Id.*

177. 709 F.3d 952 (9th Cir. 2013).

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

179. *Id.* at 1234.

180. *Id.*

The court further emphasized a distinction between searches of persons and of property in the Supreme Court's decisions on border searches.¹⁸¹ Based on Eleventh Circuit precedent, the court noted that the most important factors that determine whether someone's personal dignity was excessively degraded by a border search include "(1) physical contact between the searcher and the person searched; (2) exposure of intimate body parts; and (3) use of force."¹⁸² Unlike strip searches or even x-ray searches, the search of someone's cell phone or laptop would not implicate these concerns.¹⁸³

Finally, the court indicated its preference for Congress to regulate the limitations of border searches, not the courts.¹⁸⁴ The court stated that Congress would be better equipped than the courts "to design the appropriate standard 'through the more adaptable legislative process and the wider lens of legislative hearings.'"¹⁸⁵

In a concurring opinion, Judge Corrigan stated that he would reach the court's judgement on the narrower grounds that CBP had reasonable suspicion when they conducted the search.¹⁸⁶ Judge Corrigan would avoid reaching the "different and difficult question" of whether border agents need justification at all to detain and forensically analyze electronic devices before the Supreme Court has opined on the matter.¹⁸⁷

2. *The Fourth Circuit View: At Least Reasonable Suspicion Is Required to Forensically Search an Electronic Device at the Border*

Unlike the Court of Appeals for the Eleventh Circuit, the Court of Appeals for the Fourth Circuit recognized a clear distinction between a forensic search of the contents of a cell phone and a search of other physical property

181. *Id.* at 1233–34. The only case where the Supreme Court required reasonable suspicion for a border search was based on the extended detention of a person. *See United States v. Montoya de Hernandez*, 473 U.S. 531, 541 (1985) (requiring reasonable suspicion to detain a woman for nearly an entire day to compel her to pass contraband from her alimentary canal). Based on *Flores-Montano*, the court concluded that even invasive or lengthy searches of property did not implicate a need for heightened suspicion. *Touset*, 890 F.3d at 1233; *see United States v. Flores-Montano*, 541 U.S. 149, 155 (2004) (upholding the disassembly of a vehicle's fuel tank to search for contraband without suspicion).

182. *Touset*, 890 F.3d at 1234 (quoting *United States v. Vega-Barvo*, 729 F.2d 1341, 1346 (11th Cir. 1984)).

183. *Id.* In the alternative, the court determined that if reasonable suspicion was required to search *Touset's* electronic devices at the border, reasonable suspicion existed at the time of the search. *Id.* at 1237–38.

184. *Id.* at 1236.

185. *Id.* at 1237 (quoting *United States v. Kolsuz*, 890 F.3d 133, 150 (4th Cir. 2018) (Wilkinson, J., concurring)).

186. *Id.* at 1238–39 (Corrigan, J., concurring).

187. *Id.*

carried across the international border.¹⁸⁸ In *United States v. Kolsuz*¹⁸⁹ the Fourth Circuit announced that forensic searches of cell phones at the border require at least reasonable suspicion, if not more;¹⁹⁰ a manual search, however, is a routine border search that requires no individualized suspicion.¹⁹¹ This position mirrors the Ninth Circuit's stance regarding laptop searches at the border, which predated *Riley*, and decisions in other circuits that have required reasonable suspicion for border searches that involve more thorough inspections of property.¹⁹²

On February 2, 2016, Hamza Kolsuz, a Turkish citizen, attempted to board a plane at Washington Dulles International Airport bound for Istanbul, Turkey, when CBP agents stopped him on the jetway.¹⁹³ CBP agents had found various firearms parts in his checked luggage, some of which are illegal to remove from the United States without a specific export license.¹⁹⁴ After Kolsuz admitted he was in possession of firearms parts without a federal firearms license, CBP transported Kolsuz and his belongings to a secondary inspection area at the airport where a CBP officer conducted a manual inspection of Kolsuz's iPhone by navigating the unlocked phone's touch

188. *United States v. Kolsuz*, 890 F.3d 133, 146 (4th Cir. 2018).

189. 890 F.3d 133 (4th Cir. 2018).

190. *Id.* at 144.

191. *Id.* at 142. In *Kolsuz*, the court also clarified that when an individual is arrested at a border crossing, a search of their person and possessions are still governed by the border search exception and need not adhere to stricter guidelines governing the search incident to arrest exception. *Id.* This varies from the presentation in *Vergara* and *Touset* because in those cases, the defendant was arrested based on digital evidence found on their electronic devices. *See supra* notes 151–157 and accompanying text. *Kolsuz* could have been arrested based on the physical contraband initially discovered in his suitcase alone before officers searched his phone. *See Kolsuz*, 890 F.3d at 847–48 (stating officers immediately knew that the items found in Kolsuz's luggage could not be taken out of the country without a proper license, and Kolsuz admitted he did not have a license before being asked to hand over his cell phone).

192. *United States v. Cotterman*, 709 F.3d 952, 962 (9th Cir. 2013) (en banc), *cert. denied*, 134 S. Ct. 899 (2014). Additionally, though the United States Court of Appeals for the District of Columbia Circuit did not issue an opinion in the case, the court dismissed an appeal from the District Court for the District of Columbia that also held at least reasonable suspicion was required for a forensic cell phone search, indicating their likely adherence to the Fourth and Ninth Circuits' position. *United States v. Kim*, No. 150-3035, 2015 WL 5237696 (D.C. Cir. Aug. 14, 2015), *dismissing appeal from*, 103 F. Supp. 3d 32, 34 (D.D.C. 2015). Additionally, though the United States Court of Appeals for the Second Circuit has not ruled on what level of suspicion is required for a forensic search of a cell phone or laptop at the border, in a decision concerning the reasonableness of a border search in which agents copied and read the entire contents of a travelers handwritten journal, the court indicated that this careful reading and copying, in contrast to merely skimming or opening the notebook, could be construed as a nonroutine border search that would require reasonable suspicion. *United States v. Levy*, 803 F.3d 120, 122 (2d Cir. 2015). This careful reading distinction is analogous to a forensic search of a laptop. *Id.* (citing *United States v. Arnold*, 533 F.3d 1003, 1009 (9th Cir. 2008)). Therefore, it is likely that the Second Circuit would also determine that reasonable suspicion is required for a forensic search of an electronic device at the border.

193. *United States v. Kolsuz*, 185 F. Supp. 3d 843, 847 (E.D. Va. 2016), *aff'd*, 890 F.3d 133 (4th Cir. 2018).

194. *Id.* at 847–48.

screen to view recent text messages and phone calls.¹⁹⁵ After further investigation and questioning, CBP arrested Kolsuz and seized many of his belongings, including his smartphone.¹⁹⁶

CBP agents forensically searched the entire digital contents of Kolsuz's smartphone. The search took one month and generated an 896-page report that included Kolsuz's personal contacts list, photographs, emails, videos, conversations from messaging applications, calendar information, web browsing history, call logs, and a history of the phone's precise GPS coordinates.¹⁹⁷

The district court denied Kolsuz's motion to suppress evidence obtained from the forensic search of his phone, rejecting his argument that based on *Riley*,¹⁹⁸ the search required a warrant supported by probable cause.¹⁹⁹ The district court determined that the forensic cell phone search was a nonroutine border search, but only required reasonable suspicion.²⁰⁰ Because the CBP officers had reasonable suspicion, the search was upheld.²⁰¹

The court of appeals affirmed the district court's judgement, denying the suppression of evidence from the border search of Kolsuz's phone.²⁰² The court also agreed with the district court that a forensic search of a cell-phone at the border is a nonroutine border search, permissible only upon a showing of individualized suspicion.²⁰³ The court reasoned that the quantity of data stored on a smartphone, the sensitive nature of the information, and the fact that a traveler cannot reasonably mitigate the intrusion made the search significantly more invasive than a routine border search.²⁰⁴ The court likened the forensic search of a smartphone to other highly intrusive border searches, such as strip searches, alimentary-canal searches, and x-rays, that other courts have held require reasonable suspicion.²⁰⁵ The court noted that these conclusions were consistent with the Supreme Court's ruling in *Riley*, which limited the search incident to arrest exception's application to cell phones.²⁰⁶

195. *Id.* at 848.

196. *Id.* at 849.

197. *Id.* at 849–50.

198. 134 S. Ct. 2473, 2495 (2014).

199. *Kolsuz*, 185 F. Supp. 3d at 858.

200. *Id.*

201. *Id.* at 860.

202. *United States v. Kolsuz*, 890 F.3d 133, 148 (4th Cir. 2018).

203. *Id.* at 146. Because Kolsuz did not challenge the manual search of his phone, the court did not consider whether any individual suspicion was required for a manual search. *Id.* at 146 n.5.

204. *Id.* at 144–45.

205. *Id.* at 144.

206. *Kolsuz*, 890 F.3d at 145–46.

The court did not conclude whether reasonable suspicion, or something more, was enough to justify the forensic cell phone search.²⁰⁷ Instead, the court affirmed the district court's decision to admit evidence from the forensic search based on the good faith exception, finding that there was reasonable suspicion for the search in this case, and even if more was required, CBP officers reasonably relied on established precedent allowing warrantless border searches of digital devices based on reasonable suspicion.²⁰⁸

In a concurring opinion, Judge Wilkinson agreed with the majority's holding that the search was permissible but lamented the majority's willingness to declare the forensic search of a smartphone a "nonroutine" border search instead of reaching the same holding on more limited grounds.²⁰⁹ Judge Wilkinson stressed the important role the executive and legislative branches should play in determining the limits of the government's power in protecting the border.²¹⁰ He reasoned that those branches would have the knowledge and information available to better weigh the privacy and security interests at stake.²¹¹ Judge Wilkinson also found that the Supreme Court's ruling in *Riley* was distinguishable from the border exception and the same analysis did not apply.²¹²

3. Other Pending Challenges

Growing privacy concerns surrounding cell phones and other personal electronic devices have spurred ongoing challenges in other jurisdictions.²¹³ Although no other circuit court has issued an opinion determining the application of the border search exception to cell phones, several appeals presenting this issue are pending while other cases are making their way through the trial courts.²¹⁴ One case, in the United States District Court for the District

207. *Id.* at 148.

208. *Id.*

209. *Id.* at 148 (Wilkinson, J., concurring).

210. *Id.*

211. *Id.* at 153.

212. *Id.* at 152.

213. *E.g.*, *United States v. Molina-Isidoro*, 884 F.3d 289 (5th Cir. 2018) (declining to decide whether cell phones are outside the scope of the border search exception but allowing a cell phone search under the good faith exception); *United States v. Unpradit*, No. 17-107(4), 2018 WL 3377177, at *3 (D. Minn. July 11, 2018) (holding a manual search of a cell phone was a routine border search); *United States v. Caballero*, 178 F. Supp. 3d 1008, 1017 (S.D. Cal. 2016) (stating the court would apply *Riley* to cell phone searches at the border if it was not bound by Ninth Circuit precedent, permitting warrantless search based on reasonable suspicion); *United States v. Feiten*, No. 15-20631, 2016 WL 894452, at *4 (E.D. Mich. Mar. 9, 2016) (holding *Riley*'s warrant requirement for cell phone searches did not apply to border searches).

214. *United States v. Wanjiku*, No. 16 CR 296, 2017 WL 1304087 (N.D. Ill. Apr. 6, 2017), *argued*, No. 18-1973 (7th Cir. Nov. 7, 2018); *United States v. Cano*, 222 F. Supp. 3d 876 (S.D. Cal. 2016), *appeal docketed*, No. 17-50151 (9th Cir. Apr. 28, 2017); *United States v. Williams*, No. 16-CR-249 (D. Colo.), *appeal docketed*, No. 18-1299 (10th Cir. July 27, 2018).

of Massachusetts, seeking a declaration that DHS's electronic device policies are prohibited by the Fourth Amendment, illustrates a shifting attitude towards more protections for smartphones.²¹⁵

On September 13, 2017, ten United States citizens and one lawful permanent resident filed an amended complaint in the Federal District Court for the District of Massachusetts alleging the search and seizure of their smartphones, laptops, and other electronic devices at the border violated the Fourth Amendment.²¹⁶ All of the plaintiffs were subject to extensive searches of their personal electronic devices and none has been charged with any criminal offense.²¹⁷ The lawsuit, naming Secretary of Homeland Security Kirstjen Nielson, Acting Commissioner of U.S. Customs and Border Protection Kevin McAleenan, and Acting Director of U.S. Immigration and Customs Enforcement Thomas Homan, in their official capacity as defendants, sought injunctive and declaratory relief from the agency policies on electronic device searches.²¹⁸ The plaintiffs asked the court to declare the policies unconstitutional and to enjoin the defendants from continuing to operate in accordance with them.²¹⁹

On May 9, 2018, the district court denied the defendants' motion to dismiss the case for failure to state a claim.²²⁰ Six years earlier, the same court and judge dismissed a similar challenge to a suspicionless search of an electronic device at the international border.²²¹ This time, however, the court

215. *Alasaad v. Nielsen*, No. 17-cv-11730-DJC, 2018 WL 2170323, at *1 (D. Mass. May 9, 2018).

216. *Id.* at *1. The plaintiffs also allege the searches and seizures violated the First Amendment. *Id.* Plaintiffs are represented by attorneys from the Electronic Frontier Foundation, the American Civil Liberties Union Foundation, and the American Civil Liberties Union Foundation of Massachusetts. *Id.* The plaintiffs come from various backgrounds—among them one is a NASA engineer, one is a graduate journalism student, another an independent filmmaker, and another a former Air Force captain. *Id.* at *5–9. The plaintiffs include Ghassan Alasaad, Nadia Alasaad, Shuhaib Allababidi, Sidd Bikkannavar, Jérémie Dupin, Aaron Gach, Ismail Abdel-Rasoul, Diane Maye, Zainab Merchant, Mohammed Akram Shibly, and Matthew Wright. *Id.* at *1.

217. *Id.* at *5–9.

218. *Id.* at *1. The plaintiffs request these law enforcement agencies be enjoined from continuing to operate under their current policies, a declaration that the policies violate the Fourth and First Amendments and that the individual plaintiff's rights were violated, and that the government return the device of one plaintiff and expunge all information gathered from the plaintiffs' electronic devices and the social media information and device passwords provided. *Id.* at *9, *11.

219. *Id.* at *1.

220. *Id.* at *24.

221. *See House v. Napolitano*, No. 11-10852-DJC, 2012 WL 1038816, at *8 (D. Mass. Mar. 28, 2012) (dismissing the plaintiff's claim that his Fourth Amendment rights were violated when his electronic devices were searched at the border). The court still allowed the case to proceed on other grounds. *Id.* Ultimately, House reached a settlement with the Government in May 2013 in which the Government agreed to release documents compiled throughout their investigation of House in exchange for him to withdraw his claim. *House v. Napolitano*, ACLU (Sep. 9, 2013), <https://www.aclu.org/cases/house-v-napolitano?redirect=free-speech/house-v-napolitano>.

took notice of the Supreme Court's *Riley* decision and concluded that although the border exception presents notably different government interests than the search incident to arrest exception,²²² the court's analysis of the privacy interest at stake in smartphones in *Riley*, may impact the analysis of the border search exception enough to state a claim and allow the lawsuit to proceed.²²³

II. ANALYSIS

Judges and policymakers alike have contemplated to what extent digital property should be treated differently from physical objects being transported across the international border.²²⁴ In January 2018, the CBP issued an updated policy providing new guidance for how CBP personnel should carry out searches of electronic devices.²²⁵ Weeks later, lawmakers introduced a bill in the Senate to place additional restrictions on border searches.²²⁶ Within months, the Fifth,²²⁷ Fourth,²²⁸ and Eleventh circuits²²⁹ all ruled on cases challenging the constitutionality of electronic device searches at the border.²³⁰ Similar challenges are still pending in other circuits.²³¹ Each of these decisions articulated a different standard for when and how these searches should take place. As a result, travelers and law enforcement officers alike are faced with conflicting guidance and expectations. Still, all these events suggest that electronic devices pose different concerns than other property inspected at border crossings.

222. See *Alasaad v. Nielsen*, No. 17-cv-11730-DJC, 2018 WL2179323, at *19 (D. Mass. May 9, 2018) (noting that digital contraband “falls within the ambit of the border search exception’s rationales”).

223. *Id.* at *20.

224. See *supra* Part I.

225. See *supra* Section I.B.3.a.

226. See *supra* Section I.B.3.c.

227. *United States v. Molina-Isidoro*, 884 F.3d 287 (5th Cir. 2018) (upholding a cell phone search because agents had probable cause and even if a warrant was required, their actions would be covered by the good faith exception).

228. *United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018) (upholding a cell phone and laptop search because agents had reasonable suspicion to conduct a nonroutine search and if more was required their actions would be covered by the good faith exception).

229. *United States v. Touse*, 890 F.3d 1227 (11th Cir. 2018) (upholding a search of several electronic devices because no level of individual suspicion is required for a border search, and, in the alternative, agents had reasonable suspicion to conduct the search).

230. See *supra* Section I.C.

231. *E.g.*, *United States v. Wanjiku*, No. 16 CR 296, 2017 WL 1304087 (N.D. Ill. Apr. 6, 2017), *argued*, No. 18-1973 (7th Cir. Nov. 7, 2018); *United States v. Aigbekaen*, *appeal docketed*, No. 17-4109 (4th Cir. Feb. 23, 2017); *Alasaad v. Nielsen*, No. 17-cv-11730-DJC, 2018 WL2179323, at *1 (D. Mass. May 9, 2018).

This Part will first analyze the privacy interest that individuals crossing the border have in their cell phones and other digital devices.²³² Next, this Part will analyze what government interest is served by the border search exception and, subsequently, whether searching digital devices at the border serves this interest.²³³ Finally, this Part will ask whether establishing tiers of intrusiveness for digital searches at the border, as recommended by various courts, executive agencies, and members of Congress, appeases Fourth Amendment concerns and can be practically implemented.²³⁴

A. *The Privacy Interest in the Data on Digital Devices Greatly Exceeds That Originally Contemplated in the Border Search Exception*

Although the expectation of privacy may be diminished at a border crossing,²³⁵ travelers' privacy interests in their cell phone data remains significantly higher than in other types of property traditionally searched without suspicion at the border. The Supreme Court has recognized that ubiquitous use of smartphones has increased the potential intrusiveness of government investigations that traditionally were conducted without a warrant.²³⁶ The concerns articulated by the Court in these cases similarly arise here.

1. *Digital Property Stored on Electronic Devices Raise Different Privacy Concerns than Physical Representations of the Same Content*

The sheer amount of personal data transported in a phone, laptop, or other electronic device increases individual privacy concerns.²³⁷ Even before the digital era, the Supreme Court implied that when an extensive amount of property is searched, it may be outside the scope of a warrant exception.²³⁸ More recently in both *Riley v. California* and *Carpenter v. United States*, the Court noted that accumulation of personal data can pose increased privacy

232. See *infra* Section II.A.

233. See *infra* Section II.B.

234. See *infra* Section II.C.

235. See *United States v. Flores-Montano*, 541 U.S. 149, 154 (2003) (citing *United States v. Montoya de Hernandez*, 473 U.S. 531, 540 (1985)).

236. See *Carpenter v. United States*, 138 S. Ct. 2206, 2219 (2018) (third party doctrine); *Riley v. California*, 134 S. Ct. 2473, 2485 (2014) (search incident to lawful arrest exception).

237. *Riley*, 134 S. Ct. at 2489.

238. See *Kremen v. United States*, 353 U.S. 346, 347–48 (1957) (per curiam) (finding the search and seizure of the entire contents of the defendants' cabin upon their arrest without a warrant was not permitted).

concerns.²³⁹ Smaller amounts of personal information may be revealing in themselves, but when personal information is aggregated, further inferences about a person's life can readily be made.²⁴⁰ Cell phones and other common electronic devices often carry an incredible amount of personal data.²⁴¹ Additionally, these devices often contain different types of personal data (for example, calendars and schedules, contact lists, geolocation history, photos and videos, internet and application usage) that prove even more revealing when aggregated.²⁴²

In determining whether a forensic laptop search was reasonable, the Ninth Circuit in *United States v. Cotterman* estimated that the average laptop hard drive could store the information contained in five floors of an academic library.²⁴³ The Fourth Circuit echoed these assessments in *United States v. Kolsuz*, explaining that the quantity of data “stored on smartphones . . . dwarfs the amount of personal information that can be carried over a border . . . in luggage or a car.”²⁴⁴ After a month of extracting data from Kolsuz's phone, the government generated 896 pages of personal data.²⁴⁵ These observations imply that an individual carrying a phone or laptop has a greater privacy interest in that device than in all the other property with which they would have otherwise traditionally traveled.²⁴⁶

239. See *Riley*, 134 S. Ct. at 2489 (“The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions.”); *Carpenter*, 138 S. Ct. at 2217–18 (noting that because CSLI data is constantly recorded it provides a “deep repository of historical location information,” which shows a suspect's every movement for potentially years of his life).

240. See GRAY, *supra* note 22, at 109–16 (discussing the “mosaic theory” explanation of how aggregated data poses a greater privacy interest than the sum of an individual's interests in individual pieces of information).

241. See Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 542 (2005) (explaining a typical computer sold in 2005 with eighty gigabytes of storage roughly equated to forty million pages of text or all the books on one floor of an academic library).

242. *Riley*, 134 S. Ct. at 2489; see also James Carmichael, *Google Knows You Better Than You Know Yourself*, ATLANTIC, (Aug. 19, 2014), <https://www.theatlantic.com/technology/archive/2014/08/google-knows-you-better-than-you-know-yourself/378608/> (discussing how Google's awareness of a person's calendar, internet browsing, shopping history, and geolocation enables their software to make predictions about a person's behavior before the person themselves, such as when and where a person needs to go, what a person may need or want to buy, or what website they want to visit).

243. 709 F.3d 952, 964 (2013) (citing Kerr, *supra* note 241, at 542).

244. *United States v. Kolsuz*, 890 F.3d 138, 145 (2018).

245. *Id.*

246. See *Riley*, 134 S. Ct. at 2489 (“Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so.”). But see *United States v. Touset*, 890 F.3d 1227, 1233 (11th Cir. 2018) (reasoning that the vast amount of information on electronic devices does not indicate they should be treated differently in a border search, but rather are the same as searching “a recreational vehicle filled with personal effects or a tractor-trailer loaded with boxes of documents”).

Additionally, the nature of the data found on electronic devices increases individual privacy interests. The earliest customs statutes which authorized warrantless searches of ships and containers at ports of entry specifically distinguished this type of search from the search of homes and dwellings, which were more limited and required a warrant.²⁴⁷ In *Riley*, the Court reasoned that the kind of data discoverable on a cell phone exposes more about a person than what would be found after “ransacking his house for everything which may incriminate him.”²⁴⁸ The Court recognized that phones now contain many of the “sensitive records previously found in the home,” like medical and banking information.²⁴⁹ Indeed, given the creation of other smart devices and applications, cell phones and computers can provide a direct view into what is going on inside someone’s home.²⁵⁰ Electronic devices also often store information that may be privileged from government investigations, such as legal documents between attorneys and clients, doctor-patient records, journalist information, and spousal communications.²⁵¹

Given both the nature and quantity of the information provided by these devices, the *Riley* Court concluded that they “are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans ‘the privacies of life.’”²⁵² This assessment remains unchanged whether a device is located inside the United States or brought to the international border.

Furthermore, increasing reliance on digital devices for all aspects of day-to-day life along with increased international travel limit many individuals’ ability to reduce potential exposure to intrusive border searches.²⁵³ The Supreme Court explained in *Carpenter* and *Riley* that the pervasive use of cell phones, which have now become a “feature of human anatomy,” requires

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

248. *Riley*, 134 S. Ct. at 2490–91 (quoting *United States v. Kirschenblatt*, 16 F.2d 202, 203 (2d Cir. 1926) (Learned Hand, J.)).

249. *Id.* at 2491.

250. *See United States v. Saboonchi*, 990 F. Supp. 2d 536, 563–64 (D. Md. 2014) (describing the iCam application on iPhones that can access a web cam on a home computer, potentially allowing “the touch of a button” to turn “a cell phone search [into] a house search”); *Examining Warrantless Smartphone Searches at the Border: Hearing Before the Subcomm. on Fed. Spending Oversight and Emergency Mgmt. of the S. Comm. on Homeland Sec. & Governmental Affairs*, 115th Cong. 24 (statement of Laura K. Donohue, Agnes N. Williams Research Professor; Director, Center on National Security and the Law; and Director, Center on Privacy & Technology, Georgetown Law) [hereinafter Statement of Laura K. Donohue] (discussing the Blink Home Monitor application that allows real-time information on what is happening in someone’s house on their cell phone).

251. Statement of Laura K. Donohue, *supra* note 250, at 24–25.

252. *Riley*, 134 S. Ct. at 2494–95 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

253. *United States v. Kolsuz*, 890 F.3d 133, 145 (2018) (finding it is not “realistic nor reasonable to expect the average traveler” to not carry digital devices with them) (quoting *Saboonchi*, 990 F. Supp. 2d at 556).

them to be treated differently than other personal property.²⁵⁴ Since *Riley*, smartphone ownership has continued to grow, and today roughly eighty-five percent of Americans own a smartphone.²⁵⁵ Reliance on smartphones to assist in regular tasks has also continued to grow.²⁵⁶ Over half of smartphone owners use their device within fifteen minutes of waking up in the morning and until within fifteen minutes of going to bed at night.²⁵⁷ This increased reliance makes it implausible for users concerned with their privacy to just leave their electronic devices at home when traveling.²⁵⁸ Similarly, more people have adopted lifestyles that require travel in and out of the United States. International personal travel has become cheaper, easier, and more prevalent.²⁵⁹ The globalization of economic markets has also led to significantly increasing international business travel,²⁶⁰ which is expected to grow nearly forty percent between 2015 and 2020.²⁶¹

Overall, electronic devices are designed and used today in ways that significantly implicate an individual's privacy interests. Although expectations of privacy are less at the border than in other public spaces, it is unlikely that the Supreme Court will continue to accept the proposition that individual privacy interests in the digital content found on electronic devices should be valued the same as paper copies of the same information.²⁶²

254. *Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018) (quoting *Riley*, 134 S. Ct. at 2484).

255. DELOITTE, 2018 GLOBAL MOBILE CONSUMER SURVEY: US EDITION 7 (2018), <https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/global-mobile-consumer-survey-us-edition.html>. This is over a twenty percent increase from 2014, the year *Riley* was decided. *Mobile Fact Sheet*, PEW RES. CTR. (Feb. 6, 2018), <http://www.pewinternet.org/fact-sheet/mobile/>.

256. DELOITTE, *supra* note 255, at 4.

257. DELOITTE, 2017 GLOBAL MOBILE CONSUMER SURVEY: US EDITION 2 (2017), <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-2017-global-mobile-consumer-survey-executive-summary.pdf>.

258. *See supra* note 253.

259. *See* Max Roser, *Tourism*, OUR WORLD IN DATA (2018), <https://ourworldindata.org/tourism> (showing international tourist arrivals have continued to increase exponentially since the end of the World War II era, from 25.2 million in 1950 to 1.24 billion in 2016).

260. Per Gustafson, *Work-Related Travel, Gender and Family Obligations*, 20 WORK, EMP. & SOC'Y 513, 514 (2006).

261. *Global Business Travel Spending Growth Forecast from 2015 to 2020*, STATISTA, <https://www.statista.com/statistics/324786/global-business-travel-spending-growth-forecast/> (last accessed Mar. 10, 2019); *see also* Jordan Bishop, *Business Travel Continues to Gain in Importance*, FORBES, (Dec. 31, 2017), <https://www.forbes.com/sites/bishopjordan/2017/12/31/business-travel/#33db39385cce> (predicting business travel would grow by twenty-five percent between 2013 and 2018).

262. *Cf.* *Riley v. California*, 134 S. Ct. 2473, 2488 (2014) (“That is like saying a ride on horseback is materially indistinguishable from a flight to the moon.”).

2. *That Cell Phone Searches Are Investigations of a Traveler's Property, Not Person, Does Not Automatically Mean They Cannot Be Particularly Offensive*

The Court of Appeals for the Eleventh Circuit concluded that because border searches of electronic devices are searches of individual property, not a person's body, they are routine border searches that require no level of individualized suspicion.²⁶³ This bright line rule, however, is not clearly reflected in the Supreme Court's precedent.²⁶⁴ The Fourth Amendment is not limited to protection of "persons" but also contemplates searches of "papers, and effects."²⁶⁵ Although, the Supreme Court has not yet decided a case in which it determined a particular search of property at the border required reasonable suspicion, it has not disclosed this possibility.²⁶⁶

In *Flores-Montano*, the Court explained that disassembly and reassembly of a vehicle's gas tank was not an unreasonable search of individual property at the border.²⁶⁷ The Court, however, has never said that a search of property could not be "particularly unreasonable."²⁶⁸ Other circuits have classified border searches of property as unreasonable without individualized suspicion.²⁶⁹ Furthermore, as discussed, although electronic devices are property and not literally part of an individual "person," cell phones and other electronic devices are a distinguishable type of personal property vastly different from a vehicle fuel tank.²⁷⁰

The Eleventh Circuit first articulated three factors that "contribute to the personal indignity [of travelers]" and would indicate a border search was unreasonable in *United States v. Vega-Barvo*.²⁷¹ These factors included "(1) physical contact between the searcher and the person searched; (2) exposure

263. *United States v. Touset*, 890 F.3d 1227, 1234 (11th Cir. 2018); *United States v. Vergara*, 884 F.3d 1309, 1313 (11th Cir. 2018).

264. *United States v. Flores-Montano*, 541 U.S. 149, 154 n.2 (2004) (citing *United States v. Ramsey*, 431 U.S. at 618 n.13).

265. U.S. CONST. amend. IV; *see also* *United States v. Seljan*, 547 F.3d 993, 1014, 1017 (9th Cir. 2008) (Kozinski, C.J., dissenting) (describing the essential protection of personal papers embedded in the history of the Fourth Amendment).

266. *Flores-Montano*, 541 U.S. at 154 n.2.

267. *Id.* at 155.

268. *Id.* at 154 n.2 (leaving open the question of what an offensive border search or property might be).

269. *See, e.g.*, *United States v. Rivas*, 157 F.3d 364 (5th Cir. 1998) (finding an intrusive search of a trailer was a nonroutine border search); *United States v. Robles*, 45 F.3d 1 (1st Cir. 1995) (finding an intrusive search of a suspicious package was a nonroutine border search); *United States v. Carreon*, 872 F.2d 1436 (10th Cir. 1989) (finding an intrusive search of a camper was a nonroutine border search).

270. *See supra* Section II.A.1; *see also* *Riley v. California*, 134 S. Ct. 2473, 2484 (2014) ("[T]he proverbial visitor from Mars might conclude [cell phones] were an important feature of human anatomy."):

271. 729 F.2d 1341, 1346 (11th Cir. 1984).

of intimate body parts; and (3) use of force.”²⁷² Though certainly relevant, these factors have not been universally adopted by other circuits, or the Supreme Court, as an all-inclusive list.²⁷³ Furthermore, developments in technology since these factors were first articulated have since produced other ways individuals can be personally humiliated. Cell phones and other electronic devices often store intimate conversations, photos, and other content that if involuntarily revealed to strangers could cause excessive embarrassment.²⁷⁴ Although these indignities may not be as offensive as a strip search, the embarrassment that might be suffered is arguably more akin to a search of an individual person than that of the inner-mechanics of their vehicle.²⁷⁵

B. Searches of Electronic Devices Do Not Clearly Support the Government’s Justification for Warrantless Border Searches

The Supreme Court’s recognition in *Riley* and *Carpenter* that the nature of cell phone data raises privacy concerns to such a degree that it is beyond the reach of some traditional warrantless investigations endorses careful scrutiny of other contexts where the government regularly collects similar information without a warrant. The Court’s reasoning in *Riley* also raises the question of whether digital property should be treated differently, not only because of individual privacy concerns, but also because the government’s interests in obtaining digital content may be different than its interest in other physical items.²⁷⁶

272. See *supra* note 183 and accompanying text.

273. See *e.g.*, *United States v. Brakes*, 842 F.2d 509, 512–13 (1st Cir.1988) (listing multiple additional factors assessed to determine if a search is not routine, including “whether the suspect’s reasonable expectations of privacy, if any, are abrogated by the search”).

274. In a recent study, thirty-one percent of people worldwide admitted they shared intimate content on their phone or computer. Lianne Caetano, *Trust and Relationships in the Mobile Era*, MCAFEE (Feb. 4, 2014), <https://securingtomorrow.mcafee.com/consumer/mobile-and-iot-security/love-relationships-tech-mobile-2014/>. Sixty percent of those who did saved or stored the intimate content on their devices. *Id.* Other types of very personal data are also communicated through cell phones. People are increasingly seeking psychotherapy, emotional, and financial counseling through texting or other applications on their smartphones. See, *e.g.*, TALKSPACE, <https://www.talkspace.com/> (last visited Mar. 10, 2019) (advertising the ability to talk or text with a mental health therapist on one’s cell phone instead of going to an office for an appointment.); PENNY, <https://www.pennyapp.io/> (last visited Mar. 10, 2019) (describing a personal finance app that tracks an individual’s income and spending, and gives personal finance advice based on information obtained from banking and credit accounts).

275. See *United States v. Cotterman*, 709 F.3d 952, 966 (2013) (en banc) (calling a forensic search of a laptop a “strip search”).

276. See *Riley v. California*, 134 S. Ct. 2473, 2485–88 (2014) (determining that cell phone searches do not serve the governmental interests underlying the search incident to arrest exception).

1. *The Purpose of the Border Search Exception*

Although warrantless border search authority has been recognized since the inception of the Fourth Amendment,²⁷⁷ the practice is not without limits.²⁷⁸ In *United States v. Montoya de Hernandez*, the Court recognized that, despite the long history of the border search exception, a border inspection is akin to other modern law enforcement practices, “[t]he permissibility of [which] is judged by ‘balancing its intrusion on the individual’s Fourth Amendment interests against its promotion of legitimate governmental interests.’”²⁷⁹ As articulated in *Riley*, the governmental interests relevant to this inquiry are not to be construed so broadly as to include anything that would benefit the government.²⁸⁰ Rather, only the governmental interests that give rise to the warrant exception should be weighed in a Fourth Amendment reasonableness inquiry, to prevent an “untether[ing] of the rule from [its] justifications.”²⁸¹ The *Riley* Court concluded that the governmental interests upon which the search incident to arrest exception rests—officer safety and preservation of evidence—are not meaningfully furthered by cell phone searches.²⁸² The governmental interests supported by warrantless border searches should be similarly assessed.

The border search exception is based on the government’s important interest in controlling who and what enters its sovereign territory.²⁸³ More specifically, border searches allow the government to ensure the collection of duties on goods, stop the introduction of contraband, and prevent unlawful entry of individuals.²⁸⁴ Following the terrorist attacks that took place on September 11, 2001, courts have also found that ensuring the government is not

277. *United States v. Ramsey*, 431 U.S. 606, 616–17 (1976) (citing *Boyd v. United States*, 116 U.S. 616, 623 (1886)).

278. *See United States v. Montoya de Hernandez*, 473 U.S. 531, 540–41 (1985) (citing *Ramsey*, 431 U.S. at 618 n.13) (explaining that some border searches require individualized suspicion).

279. *Id.* at 537 (first citing *United States v. Villamonte-Marquez*, 462 U.S. 579, 588 (1983); then citing *Delaware v. Prouse*, 440 U.S. 648, 654 (1979); and then citing *Camara v. Municipal Court*, 387 U.S. 523, 536–37 (1967)).

280. *See Riley*, 134 S. Ct at 2484–85 (determining whether a cell phone search supports the specific legitimate governmental interests that justify the search incident to arrest exception).

281. *Id.* at 2485.

282. *Id.* at 2485–88.

283. *United States v. Flores-Montano*, 541 U.S. 149, 152–53 (2004) (citing *Ramsey*, 431 U.S. at 619) (“The Government’s interest in preventing the entry of unwanted persons and effects is at its zenith at the international border.”).

284. *See, e.g., id.* (stating the executive branch may conduct warrantless border searches “in order to regulate the collection of duties and to prevent the introduction of contraband”) (quoting *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985)); *Ramsey*, 431 U.S. at 618 (“[N]ational self protection reasonably require[s] one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in.” (emphasis omitted) (quoting *Carroll v. United States*, 267 U.S. 32, 45 (1925))); *United States v. 12 200–Ft. Reels of Super 8MM Film*, 413 U.S. 123, 125 (1973) (recognizing that border search authority is justified by the need to prevent smuggling and enforce import restrictions); *Almeida-Sanchez v.*

hindered in its ability to stop terrorists or their weapons from entering the country justifies the border exception.²⁸⁵ The border search, however, is not definitely excluded from the warrant requirement in the interest of uncovering evidence of any criminal activity.²⁸⁶

In one of its earliest opinions discussing warrantless border searches, the Court specifically distinguished between the search and seizure of dutiable goods and contraband, and the search and seizure of papers that could be used as evidence of unlawful activity, declaring that while the former was permitted, the latter violated the Fourth Amendment.²⁸⁷ Although this “mere evidence rule,” which had been broadly applied to other types of searches and seizures, was abandoned by the Court in 1967,²⁸⁸ the discussion in *Boyd* reflects that the traditional justification for warrantless border searches was to uncover prohibited items or those subject to duties entering the country.²⁸⁹

United States, 413 U.S. 266, 272, (1973) (discussing the power to exclude aliens from entering this country); *United States v. Thirty-Seven Photographs*, 402 U.S. 363, 376 (1971) (explaining customs officials inspections are “an old practice . . . intimately associated with excluding illegal articles from the country”); *see also Ramsey*, 431 U.S. at 621 (rejecting the proposition that the border exception is not based on the exigent circumstances).

285. In March 2003, portions of other federal agencies including the U.S. Customs Service, immigration inspectors, agriculture inspectors, and border patrol agents combined to form CBP, which moved all of these previously separate responsibilities under the newly created DHS. *CBP Through the Years*, U.S. CUSTOMS & BORDER PROTECTION, <https://www.cbp.gov/about/history> (last modified Nov. 8, 2017). Since then, CBP has declared one of its primary tasks is to “keep[] terrorists and their weapons out of the U.S.” *About CBP*, U.S. CUSTOMS & BORDER PROTECTION, <https://www.cbp.gov/about> (last modified Nov. 21, 2016). Arguably, this does not radically change the traditional role of screening travelers for lawful status to enter the country and identifying weapons and other contraband at the border. Courts have avoided trying to answer what other specific role can or should CBP play in preventing terrorism but have often been deferential to the government’s interest in conducting a search when terrorist activity is potentially involved. *See, e.g., Tabaa v. Chertoff*, 509 F.3d 89, 92 (2d Cir. 2007) (recognizing CBP may detain and search based on “the compelling governmental interest in preventing potential terrorists from entering the United States”); *United States v. Ickes*, 393 F.3d 501, 506 (4th Cir. 2005) (raising concerns about the need to uncover “terrorist communications” or “terrorist plans” during a border search).

286. *United States v. Seljan*, 547 F.3d 993, 1015 (9th Cir. 2008) (Kozinski, J., dissenting) (“Using border searches for a purpose unrelated to border control—such as general crime prevention—raises a wholly different issue.”). Some courts have concluded that where evidence of a crime is found while conducting a legitimate border search for contraband, it may properly be seized. *See, e.g., United States v. Schoor*, 597 F.2d 1303, 1306 (9th Cir. 1979) (holding customs officials could seize documents found searching individuals arrested for suspected heroin trafficking). This kind of search, however, is often allowable based on the search incident to arrest exception or the plain view doctrine and need not be construed as part of the border search exception. *See id.* at 1306–07 (noting the customs agents seized the documents “incident to a lawful arrest”).

287. *Boyd v. United States*, 116 U.S. 616, 623 (1886).

288. *Warden, Maryland Penitentiary v. Hayden*, 387 U.S. 294, 309–10 (1967).

289. *Boyd*, 116 U.S. at 622–23; Statement of Laura K. Donohue, *supra* note 250, at 11. This is also consistent with the Court’s discussion of the border search in *Carroll v. United States*, in which the court noted it would be appropriate for any car to be stopped at the border in order for government agents to ensure it was not transporting liquor or other contraband. *Carroll v. United States*, 267 U.S. 132, 154 (1925).

The Court's holding in *United States v. Ramsey*, allowing the opening of international mail suspected of containing contraband, is consistent with endorsing a limited purpose of the border search exception.²⁹⁰ The Court explained that envelopes subject to search when carried across the border would be subject to the same search criteria if they were mailed from abroad because "[i]t is their entry into this country from without it that makes a resulting search 'reasonable.'"²⁹¹ As noted by the Court, however, the search in question was conducted in accordance with federal statutes and regulations which required reasonable suspicion that contraband was inside the envelope to initiate the search and explicitly prohibited customs personnel from reading any of the correspondence without a warrant.²⁹² The search was conducted to ensure no illegal drugs were smuggled between papers, not to see, for example, if the papers contained a letter describing a rendezvous location for a future drug transaction.²⁹³ In his concurrence, Justice Powell further emphasized the significance of the statutory preconditions in the case, stating that the statute adequately protected individual's Fourth Amendment rights.²⁹⁴ Other warrantless border searches upheld by the Supreme Court since, were conducted with the purpose and effect of discovering illegal materials from being brought into the country.²⁹⁵

A cell phone search will not uncover goods to which duties are owed or other physical contraband.²⁹⁶ Cell phones and other digital devices similarly do not carry agricultural pests, and an examination of their digital content will not reveal drugs, weapons, or other immediate threats of physical

290. *United States v. Ramsey*, 431 U.S. 606, 619 (1976).

291. *Id.* at 620.

292. *Id.* at 611, 623. Today, federal regulations continue to limit customs officers' ability to open and read international mail. See 19 C.F.R. § 145.3 (2018) (allowing customs officers to open sealed letter class mail only if they have reasonable cause to suspect the presence of merchandise or contraband and prohibiting customs officers from reading any correspondence without a warrant or the written consent of the sender or addressee).

293. *Ramsey*, 431 U.S. at 609. A customs officer first noticed the envelopes, mailed from a known drug source country, seemed bulky, felt like there was something other than paper inside, and weighed three to six times the normal weight of a letter before opening them. *Id.*; see also *United States v. Seljan*, 547 F.3d 993, 1015 (9th Cir. 2008) (Kozinski, J., dissenting) ("The case did not involve reading anything within the envelopes, nor did it involve an effort to obtain evidence of criminal activity unconnected to the customs laws.").

294. *Ramsey*, 431 U.S. at 625 (Powell, J., concurring). Justice Powell agreed to join the majority opinion only if the precedential effect of the decision should be confined to international mail searches conducted in accordance with the statute. *Id.* Justice Powell also noted the statute protected individual First Amendment rights as well. *Id.*

295. See *United States v. Flores-Montano*, 541 U.S. 149, 150 (2004) (upholding a warrantless search that led to the discovery of illegal drugs in the gas tank of an automobile); *United States v. Montoya de Hernandez*, 473 U.S. 531, 532-33 (1985) (holding that a search that led to the discovery of illegal drugs in the alimentary canal was valid).

296. *United States v. Vergara*, 884 F.3d 1309, 1317 (11th Cir. 2018) (Pryor, J., dissenting) ("[C]ell phones do not contain the physical contraband that border searches traditionally have prevented from crossing the border.").

harm.²⁹⁷ Digital contraband, including child pornography, can be obtained in searches of cell phones and electronic devices.²⁹⁸ However, CBP policy and practices do not distinguish between conducting a search based on suspicion that there is digital contraband present from suspicion that there is “activity in violation of the laws enforced or administered by CBP” or, even more broadly, suspicion that there is “a national security concern.”²⁹⁹

Although lower courts have generally embraced a broad understanding of the “national sovereignty” interest justifying warrantless border searches, contemporary law enforcement practices have pushed its limits.³⁰⁰ Some lower courts have determined that a government agent at the border could read the entire contents of an individual’s diary in order to find evidence of criminal activity under the border exception.³⁰¹ Others, though, have concluded that an interest in uncovering evidence alone is not close enough to the reasons underlying the border search exception to justify a suspicionless search, especially where individual privacy interests are particularly elevated.³⁰² As the intimate details about peoples’ lives, privileged and other sensitive information are increasingly transported across the border in digital devices, it is worth considering for what purposes the government should be given unquestionable access.³⁰³ An unchecked, unlimited ability to access

297. *Cf.* *Riley v. California*, 134 S. Ct. 2473, 2485–86 (2014) (explaining that digital data cannot itself cause harm to arresting officers).

298. *E.g.*, *United States v. Touset*, 890 F.3d 1227, 1235 (2018) (explaining that the government’s interest in stopping contraband from entering the country does not depend on whether the illegal images are digital or physical photographs).

299. *See* CBP DIRECTIVE NO. 3340-049A, *supra* note 115.

300. Two circuits have upheld searches in which CBP searched and seized personal documents from travelers who were being investigated for financial crimes unrelated to international customs law, immigration, terrorism, or their travel abroad by the FBI during a border search. *United States v. Levy*, 803 F.3d 120, 121 (2d Cir. 2015); *United States v. Gurr*, 471 F.3d 144, 147–50 (D.C. Cir. 2006). As the CBP has become more integrated with other law enforcement agencies, potential to investigate travelers for unrelated activity has grown. *See Law Enforcement Information Sharing*, OFFICE OF THE DIR. OF NAT’L INTELLIGENCE, <https://www.dni.gov/index.php/who-we-are/organizations/ise/ise-archive/ise-additional-resources/2142-law-enforcement-information-sharing> (last visited Mar. 10, 2019) (describing how information sharing among all law enforcement agencies has significantly expanded to better combat threats of terrorism, but the same advancements “are also applicable to other types of crime”).

301. *United States v. Blackwell*, No. 19-CR-0138, 2018 WL 6804803, at *5 (D. Minn. Dec. 27, 2018); *United States v. Saboonchi*, 990 F. Supp. 2d 536, 563 (D. Md. 2014).

302. *United States v. Kim*, 103 F. Supp. 3d 32, 59 (D.D.C. 2014), *appeal dismissed*, No. 15-3035, 2014 WL 5237696 (D.C. Cir. Aug. 14, 2015).

303. *United States v. Molina-Isidoro*, 884 F.3d 287, 296 (5th Cir. 2018) (Costa, J., concurring) (“If contraband is not being electronically concealed in phones and computers, does the government still have as compelling an interest in searching those items at the border?”).

individual's personal information could potentially allow for abuse of this process and contradict constitutional values.³⁰⁴

2. *Border Searches Used to Investigate Unrelated Activity*

CBP's broad policy, allowing extensive warrantless searches of electronic devices, yielding potentially hundreds of pages of personal data, whenever there is a hunch that any illegal activity is ongoing, certainly makes the border search appear as if it can be used for general policing.³⁰⁵ Other searches conducted pursuant to different special needs warrant exceptions have been struck down based on a showing that despite other cursory purposes, the "central and indispensable feature" of the search regime was for general law enforcement.³⁰⁶ As discussed above, it is far from clear that a general law enforcement or evidence-gathering purpose underlies the border exception.³⁰⁷

Still, even if the border search exception is construed to support a broad national security purpose, the common law enforcement technique of tagging individuals for search at the border seems to contradict the veracity of the "national security" justification.³⁰⁸ In several cases, a law enforcement or intelligence agency flags an individual's name as associated with some other investigatory interest in a shared database.³⁰⁹ However, instead of further

304. In his opening statement in the U.S. Senate Subcommittee on Federal Spending Oversight and Emergency Management hearing on smartphone searches at the border, Ranking Member Senator Gary C. Peters described concerns that current CBP policies function as a "backdoor travel ban," unfairly impacting Arab and Muslim-Americans, create "an immense disincentive to travel," "hurt[] families," and "impact[] commerce." *Examining Warrantless Smartphone Searches at the Border: Hearing Before the Subcomm. on Fed. Spending Oversight and Emergency Mgmt. of the S. Homeland Sec. and Governmental Affairs Comm.*, 115th Cong. 2 (2018) (statement of Sen. Peters, Ranking Member, Subcomm. on Fed. Spending Oversight and Emergency Mgmt.).

305. See CBP DIRECTIVE NO. 3340-049A, *supra* note 115; *United States v. Vergara*, 884 F.3d 1309, 1317 (11th Cir. 2018) (Pryor, J., dissenting).

306. *Ferguson v. City of Charleston*, 532 U.S. 67, 69–70, 80 (2001) (finding drug testing of pregnant women and reporting results to police without the patient's consent or a warrant was unconstitutional); *United States v. Bulacan*, 156 F.3d 963, 967–68, 974 (9th Cir. 1998) (deciding administrative search scheme that allowed the government to search any personal belongings carried into a federal building, not only for weapons or explosives but for anything violating federal regulations including drug paraphernalia, was unconstitutional).

307. See *supra* Section II.B.1; see also *Vergara*, 884 F.3d at 1317 (Pryor, J., dissenting) (finding a general law enforcement purpose for border searches "quite far removed" from the purpose of the warrant exception); see also *United States v. Molina-Isidoro*, 884 F.3d 287, 297 (5th Cir. 2018) (Costa, J., concurring) (noting the Supreme Court has not commented much about the alternative justification for the border search as a tool for protecting "national security").

308. See *United States v. Kim*, 103 F. Supp. 32, 57 (D.D.C. 2015) (questioning how national security concerns can underlie a warrantless forensic laptop search at the border where the owner "posed so little of an ongoing threat to national security, that he was permitted to board his flight").

309. U.S. DEP'T OF HOMELAND SEC., *TECS SYSTEM: PLATFORM 18* (2016). TECS is an information sharing platform used and managed by CBP that allows multiple federal law enforcement agencies to use and record information about potential travelers that may raise a security concern.

pursuing the individual, the government may wait until the individual arrives at a border crossing, then seize and extensively search their electronic devices and other property.³¹⁰ In other cases, where an individual is suspected of a crime, the government has used the border search authority of CBP to access information or records the agency would not otherwise have access to if they were inside the country, even where the investigation is for a crime unrelated to the individual's international travel, customs laws, immigration, or terrorism.³¹¹ Certainly, the government should not be discouraged or thwarted in its ability to pursue credible complex threats to our nation's security. International travel, however, should not provide a loophole to Fourth Amendment protections and allow the government to seize personal information unrelated to the justifications embedded in general sovereignty interests at the border.³¹² Additionally, electronic files that may implicate a criminal plan or conspiracy that threatens national security may be regulated or obtained by other means and may not actually present such a compelling reason to allow intrusive warrantless searches of electronic devices at the border.³¹³

Id. at 1. FBI personnel input information indicating an individual is suspected of involvement in a violation of federal law and what if any actions should be taken by CBP if and when that person attempts to cross the border. *Id.* at 18.

310. In one case, David House, a U.S. citizen, was working with the Bradley Manning Support Network to raise legal defense funds for a soldier who has since pleaded guilty to providing classified documents to WikiLeaks. Brian Hauss, *Documents Shed Light on Border Laptop Searches*, ACLU (Sep. 9, 2013), <https://www.aclu.org/blog/national-security/privacy-and-surveillance/documents-shed-light-border-laptop-searches>. Although he was not questioned by law enforcement officers in the United States, a lookout was placed in the TECS database stating that he was wanted for questioning about a leak of classified material. *Id.* The lookout further stated that customs officers should conduct a full secondary inspection of him and his bags and secure his digital media. *Id.* When he returned from a vacation in Mexico to Chicago O'Hare International Airport, he was questioned by CBP and his laptop was seized and searched. *Id.* House later filed a lawsuit alleging the government's action violated the Fourth and First Amendments. *Id.* The government reached a settlement with House in 2013 in which the government agreed to turn over information they had gathered about House. *Government Documents Released Under House v. Napolitano Settlement*, ACLU (Sep. 9, 2013), <https://www.aclu.org/legal-document/government-documents-released-under-house-v-napolitano-settlement>.

311. In one case, a traveler was being investigated by the Drug Enforcement Agency ("DEA") for securities fraud. *United States v. Levy*, 803 F.3d 120, 121 (2d Cir. 2015). When he returned to the United States from a trip abroad, his notebook was searched and copied by customs agents in support of DEA's ongoing investigation. *Id.* In another case, several financial documents were searched and seized from a traveler at an international airport who was suspected of credit union fraud. *United States v. Gurr*, 471 F.3d 144, 150 (D.C. Cir. 2006).

312. Susan Stellin, *The Border Is a Back Door for U.S. Device Searches*, N.Y. TIMES (Sept. 9, 2013), <https://www.nytimes.com/2013/09/10/business/the-border-is-a-back-door-for-us-device-searches.html>.

313. See Statement of Laura K. Donohue, *supra* note 250, at 23–24 (discussing the ability for the government to obtain digital contraband through other means and that such matters may fall within the scope of the Foreign Intelligence Surveillance Act); see also *United States v. Vergara*, 884 F.3d 1309, 1317 (11th Cir. 2018) (Pryor, J., dissenting) (questioning whether border searches are the best means of obtaining "borderless" digital content).

C. Tiers of Intrusiveness

The Fourth and Ninth Circuits and CBP have endorsed policies that distinguish two types of electronic device border searches: manual or basic searches, which do not require individualized suspicion, and forensic or advanced searches, which require reasonable suspicion.³¹⁴ Proposed legislation in the Senate takes on a similar format, proscribing more stringent requirements for forensic searches than for manual searches.³¹⁵ It is not clear, however, that either of these proposed plans rely upon meaningful, workable distinctions.

1. Problems with Creating a Tiered Search Scheme

Drawing distinctions between levels of intrusiveness for digital device searches may become an impractically difficult task as technology quickly changes. The Supreme Court expressly rejected the government's proposition in *Riley* to allow at least *less intrusive* searches of cell phones without a warrant.³¹⁶ The Court first noted that law enforcement officers are best served by clear rules on what types of searches are permissible.³¹⁷ The Court also reasoned that if a more flexible rule was adopted, as the law was being litigated, it would be hard to reach a point of clarity because the nature of electronic devices used by Americans will continue to change.³¹⁸

Additionally, although CBP's current distinction between what constitutes a basic or advanced search may be administrable, it does not conclusively reflect the level of intrusiveness actually at stake.³¹⁹ The CBP policy considers a search assisted by electronic hardware, where presumably large amounts of files can be extracted from an electronic device, to be more intrusive than a search conducted by customs agents for an indefinite period of time in or out of the presence of the device owner.³²⁰ The current distinction appears to turn on how much data can be extracted from the device, however, because the standard does not limit the amount of time an agent may search

314. *United States v. Kolsuz*, 890 F.3d 843, 858 (4th Cir. 2018); *United States v. Cotterman*, 709 F.3d 952, 967–68 (9th Cir. 2013); *see* CBP DIRECTIVE NO. 3340-049A, *supra* note 115.

315. S. 2462, 115th Cong. (2018); *see supra* notes 129–137 and accompanying text. Notably, the proposed legislation delineates two tiers that require either reasonable suspicion (“manual search”) or probable cause and a warrant (“forensic search”). S. 2462 § 2. Whereas, the CBP policy calls for no level of suspicion (“basic search”) or reasonable suspicion (“advanced search”). CBP DIRECTIVE NO. 3340-049A, *supra* note 115, ¶¶ 5.1.3–4.

316. *Riley v. California*, 134 S. Ct. 2473, 2492–94 (2014).

317. *Id.* at 2497.

318. *Id.*

319. *United States v. Kolsuz*, 890 F.3d 133, 146 (4th Cir. 2018) (reasoning that CBP's adoption of differentiating between manual and forensic searches, as recognized by the courts in *United States v. Cotterman* and *United States v. Saboonchi*, suggests that it is a “perfectly manageable” distinction).

320. CBP DIRECTIVE NO. 3340-049A, *supra* note 115, at 4–5.

a device during a basic or manual search, it is unclear that proposition will always be true.³²¹ Further, as discussed in *Riley*, even manual searches can be extremely revealing.³²² As the digital forensic technology industry continues to grow, it is possible that extrinsic tools used to search the contents of a device may work more quickly, in a more targeted manner, and may perhaps become less intrusive than a human agent combing through and viewing individual records on someone's phone.³²³

Furthermore, the distinction between manual searches and searches conducted with the assistance of other electronic tools cuts against law enforcement best practices.³²⁴ Digital forensic experts agree that manually sifting through files on someone's device is not a "forensically sound" practice because it can affect the content and state of the device.³²⁵ In order to ensure any evidence held on a cell phone can be properly admitted at a later trial, best practices advise that the original files and device should be minimally handled by investigators.³²⁶ Where it is necessary to access original digital evidence, only a person specifically trained for that purpose should do so and carefully document their actions.³²⁷

Manual searches are also less preferable because it is more difficult to ensure only data that is actually on the device is searched and data stored on servers elsewhere is not inadvertently accessed.³²⁸ Because data stored remotely is not actually carried across the border, it cannot be obtained based on the border search exception.³²⁹ The current CBP policy instructs officers to ask travelers to put their device in airplane mode or try to do so themselves

321. Cf. S. 2462, 115th Cong. (2018) (describing any search that takes longer than four hours as a forensic search).

322. *Riley*, 134 S. Ct. at 2489–91 (discussing privacy concerns that arise during the manual search of a cell phone).

323. See *United States v. Wanjiku*, No. 16 CR 296, WL 1304087, at *3 (M.D. Ill. Mar. 6, 2017) (describing encase software that can generate a preview of only the photos stored on a phone in less than an hour). See generally *EnCase Mobile Investigator Product Overview*, OPENTEXT, <https://www.guidancesoftware.com/document/product-brief/encase-mobile-investigator-product-overview> (last visited Jan. 12, 2019).

324. *Wanjiku*, WL 1304087, at *4 (“[Y]ou can’t just go on a phone and start tapping around and going through things because you affect the phone.”).

325. Rodney McKemish, *When Is Digital Evidence Forensically Sound?*, in *ADVANCES IN DIGITAL FORENSICS IV*, at 3–15 (Indrajit Ray & Sujeet Shenoj eds., 2008).

326. *Id.*

327. *Id.*

328. Cf. *Riley v. California*, 134 S. Ct. 2473, 2491 (2014) (“[O]fficers searching a phone’s data would not typically know whether the information they are viewing was stored locally . . . or has been pulled from the cloud.”).

329. Cf. *id.* (explaining that searching files stored on the cloud could not be permitted by the search incident to arrest exception). Allowing the government to search files on the cloud would be like “finding a key in a suspect’s pocket and arguing that it allowed law enforcement to unlock and search a house.” *Id.*

before searching it to block access to remotely stored data.³³⁰ This, however, could prove difficult where travelers are not cooperative or in cases where inspectors are not familiar with the functionality of individual devices. External forensic tools are designed with more precision to only download contents actually stored on the device.³³¹

2. A Warrant Requirement Will Ensure Access Only to Data That Is Constitutionally Permissible

Requiring a warrant supported by probable cause for cell phone searches at the border is an administrable requirement that adequately protects privacy interests.³³² Though some judges have suggested that it is best to let the executive branch or legislature develop policies that serve the government's interest at the border,³³³ in *Riley*, the Court expressly rejected the same argument stating, “[T]he Founders did not fight a revolution to gain the right to government agency protocols.”³³⁴ Though it may impede law enforcement some, as noted in *Riley*, technology advancements have also made getting a warrant quicker and easier.³³⁵ Furthermore, though courts have differed in their determination of what standard should be applied to electronic device searches at the border, no challenge to a search in any of the four cases decided by the circuit courts in 2018 actually excluded the evidence against a criminal defendant because the courts ultimately concluded that, even without a warrant, a requisite level of individualized suspicion was present at the time of the search.³³⁶ This suggests that in the limited number of cases where cell phone searches are helpful to carry out CBP's mission, officers may often be able to obtain the probable cause standard.³³⁷ Additionally, officers may

330. See CBP DIRECTIVE NO. 3340-049A, *supra* note 115, ¶ 5.1.2.

331. *United States v. Wanjiku*, No. 16 CR 296, WL 1304087, at *3 (M.D. Ill. Mar. 6, 2017) (explaining how devices allow agents to only access specific data); see CELLEBRITE, DATA SHEET: CENTRAL MANAGEMENT SYSTEM (2018), https://cf-media.cellebrite.com/wp-content/uploads/2018/08/DataSheet_CMS_LTR_02Aug2018.pdf (describing how Cellebrite digital forensic products allow managers to ensure policies are enforced for all users).

332. See GRAY, *supra* note 22, at 215.

333. *United States v. Touse*, 890 F.3d 1227, 1237 (11th Cir. 2018); *United States v. Kolsuz*, 890 F.3d 133, 148 (4th Cir. 2018) (Wilkinson, J., concurring).

334. *Riley*, 134 S. Ct. at 2491.

335. *Id.* at 2493 (discussing how in some jurisdictions police officers can obtain a warrant from a judge via email in less than fifteen minutes).

336. See *Touse*, 890 F.3d at 1237 (finding at least reasonable suspicion was present); *Kolsuz*, 890 F.3d at 148 (same); *United States v. Vergara*, 884 F.3d 1309, 1313 (11th Cir. 2018) (deciding no level of suspicion was required, but noting that the defendant did not challenge the lower court's finding that at least reasonable suspicion existed); *United States v. Molina-Isidoro*, 884 F.3d 287, 292 (5th Cir. 2018) (finding probable cause was present).

337. Compare *United States v. Montoya de Hernandez*, 473 U.S. 531, 541 (1985) (explaining that “inspectors will rarely possess probable cause” to search alimentary canal smugglers), with *Molina-Isidoro*, 884 F.3d at 287 (determining officers had probable cause to search the cell phone of a traveler based on her illogical responses to the officer's questions, her inconsistent travel plans,

still rely on other warrant exceptions at the border, including exigent circumstances to expediently search the contents of a phone when necessary conditions are present.³³⁸

III. CONCLUSION

The Supreme Court's recent examination of cell phone searches in traditional warrantless investigations raises the question of whether cell phone searches under other warrant exceptions should be reevaluated as well, including the border search exception.³³⁹ As legal challenges to electronic device searches at the border continue to arise, courts should recognize their significant intrusion on individual privacy and tenuous relationship with the traditional justification for the border search exception.³⁴⁰ Though some courts and policymakers have proposed creating levels of electronic device searches that would require different degrees of suspicion, this approach may present distinctions that do not always mirror the privacy interests at stake and may discourage the use of best practices for searching digital content.³⁴¹ Alternatively, imposing a warrant requirement to search personal electronic devices at the border would avoid these problems and give clear guidance to law enforcement.³⁴²

and finding methamphetamines in her suitcase), *and Kolsuz*, 890 F.3d at 148 (finding officer's had at least reasonable suspicion based on the illegal firearms parts found in the defendant's luggage and his admission that he did not have an export license, but not engaging in a probable cause analysis).

338. *Vergara*, 884 F.3d at 1317 (Pryor, J., dissenting) (citing *Riley*, 134 S. Ct. at 2494).

339. *See supra* Section II.A.

340. *See supra* Section II.B.

341. *See supra* Section II.C.1.

342. *See supra* Section II.C.2.