University of the Pacific Law Review

Volume 51 | Issue 1 Article 4

1-1-2019

The Constitutionality of Forensic Searches of Electronic Devices at the United States Border

Hayley E. Graves

The Constitutionality of Forensic Searches of Electronic Devices at the United States Border

*Hayley E. Graves**

TABLE OF CONTENTS

* J.D. and MPA Candidate, University of the Pacific, McGeorge School of Law, to be conferred May 2020; B.A. Political Science, Southern Methodist University, 2016. I first would like to thank my incredible mentors: Jean Hobler, Rick Lewkowitz, Tate Davis, and Rebecca Whitfield—you are all the attorneys I one day hope to become. Next, I would like to thank every person on law review—it takes a village of highly-motivated, creative, and intelligent people to run a law review and you all do it so well. Finally, thank you to my family, especially my inspiring siblings, Alexander, Elizabeth, and Aaron. And of course, thank you to my best friend, Michael Hopkins.

I. INTRODUCTION

You land at your hometown airport after taking a trip abroad when suddenly, a United States federal agent starts barking orders at you: *Give me your phone*.[1] *Give me your laptop*.[2] *Give me your camera.*[3] *Sit here*.[4] Confused and scared, you do what you are told.[5] You watch as the officer looks through your pictures, text messages, and emails.[6]

When you finally get the courage to ask why, the response is: *this is a border of the United States—a reason is not required to search your personal electronics.*[7] Next, you hear: *I am going to retain your electronic devices.*[8] *They will be transported to an off-site facility and forensically searched*.[9] *Thank you for crossing the United States border.*[10]

From there, you later learn federal agents took your electronic devices to an off-site facility to make an exact copy of all the data on your electronic devices—including all your deleted files.[11] At the off-site facility, officers could spend

1. *See* Matt Novak, *9 Horror Stories From People Who Had Their Electronic Devices Searched at the Border*, GIZMODO (Oct. 9, 2017), https://gizmodo.com/9-horror-stories-of-people-who-had-their-electronic-dev-1818730022 (on file with *The University of the Pacific Law Review*) (recounting stories of Customs and Border Patrol taking individual's phones and searching them).

2. *See id.* (recounting stories of Customs and Border Patrol taking individual's laptops and searching them).

3. *See id.* (recounting stories of Customs and Border Patrol taking individual's cameras and searching them).

4. *See id.* (recounting stories of Customs and Border Patrol making individual's sit and watch agents search their electronic devices).

5. *See id.* (recounting stories of Customs and Border Patrol making individual's sit and watch agents search their electronic devices).

6. *See id.* (recounting stories of Customs and Border Patrol taking individual's electronic devices, searching through the content of the devices, and question individuals about the contents).

7. *See* United States v. Ramsey, 431 U.S. 607, 616 (1977) (holding that border searches are reasonable because they are conducted at the border).

8. *See* Novak, *supra* note 1 (recounting stories of Customs and Border Patrol retaining individual's electronic devices after they are free to go).

9. *See* United States v. Kolsuz, 890 F.3d 133, 141 (4th Cir. 2018) (holding a forensic search of an electronic device at an off-site facility away from the initial stop was constitutional because law enforcement had individualized suspicion for the forensic search).

10. *See* United States v. Touset, 890 F.3d 1227, 1234 (11th Cir. 2018) (holding no suspicion is required to forensically search an electronic device at the border).

11. *See* United States v. Saboonchi, 990 F. Supp. 2d 536, 546–47 (D.D.C. 2014) (discussing how border searches may be conducted away from the border).

months combing through all your data.[12] In technical words, the United States can conduct a forensic search of your electronic devices without having any suspicion to do so.[13]

The above encounter is legal at any border within the Eleventh Circuit's jurisdiction.[14] This scenario is a reality for travelers coming in and out of the numerous airports and seaports in the Eleventh Circuit.[15] This jurisdiction includes Hartsfield-Jackson Atlanta International Airport, the busiest airport in the world with 104 million travelers in 2017.[16] The above situation exists because Eleventh Circuit precedent declares forensic searches and seizures without any suspicion constitutional when initiated at any border.[17]

Congress and the Judicial Branch of the United States have limited protections at borders since the founding of this country.[18] Both branches have allowed a lower level of protection at borders because of the desire to secure the border.[19] A circuit split has emerged, creating different levels of individualized protections against forensic searches of electronic devices at the border.[20]

The law is clear in the United States; law enforcement agents are allowed to *manually* search any electronic devices without any level of suspicion at a border.[21] Additionally, such searches and seizures happen frequently.[22] Law enforcement can lawfully conduct manual searches of electronic devices at the border without a warrant, a showing of probable cause, or even reasonable suspicion to stop (seize) an individual.[23] The jurisdictional split occurs when law

12. *See* Kolsuz, 890 F.3d at 141(holding a forensic search of an electronic device at an off-site facility away from the initial stop was constitutional because law enforcement had individualized suspicion for the forensic search).

13. *See* United States v. Feiten, No. 15-20631, 2016 WL 894452, at *6 (E.D. Mich. Mar. 9, 2016) (describing OS Triage as a software the government uses to make an exact copy of an electronic device in order to conduct a forensic search of the device).

14. *See* Touset, 890 F.3d at 1234 (holding that no suspicion is required to forensically search an electronic device at the border).

15. Maureen O'Hare, *The World's Busiest Airports in 2017 Revealed*, CNN (Apr. 9, 2018), https://www.cnn.com/travel/article/worlds-busiest-airports-preliminary 2017/index.html (on file with *The University of the Pacific Law Review*); *see also* Touset, 890 F.3d at 1234 (holding that no suspicion is required to forensically search an electronic device at the border).

16. O'Hare, *supra* note 15.

17. *See* Touset, 890 F.3d at 1234 (holding that no suspicion is required to forensically search an electronic device at the border).

18. *See* United States v. Ramsey, 431 U.S. 607, 616 (1977) (holding border searches are reasonable because they are conducted at the border).

19. *See id.* (holding that border searches are reasonable because they are conducted at the border).

20. *Infra* Part IV.

21. *See* United States v. Flores-Montano, 541 U.S. 149, 149 (2004) ("Congress has always granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country.").

22. Novak, *supra* note 1.

23. *See* Flores-Montano, 541 U.S. at 149 ("Congress has always granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country.").

enforcement conducts a *forensic* search of electronic devices at the border.[24] A forensic search occurs when a computer program is connected to an electronic device, and the program creates an exact copy of the electronic device.[25] This program makes exact copies of all saved, viewed, and deleted data, starting with the very first piece of information viewed on the device.[26] These devices include cellphones, computers, and cameras.[27]

In all jurisdictions but one, where a Court of Appeals has ruled on this issue, law enforcement agents at United States borders are required by law to have some level of suspicion to conduct a forensic search.[28] The Ninth Circuit requires reasonable suspicion for forensic searches of electronic devices at the border.[29] In addition, the Fourth Circuit requires some level of individualized suspicion to do the same forensic search.[30] Both levels of suspicion require specific facts that lead law enforcement to believe the electronic device possibly contains criminal evidence.[31]

The Eleventh Circuit rejected the Ninth and Fourth Circuits' limitations.[32] The Eleventh Circuit does not require any level of suspicion before conducting forensic searches of electronic devices at the border.[33] The Eleventh Circuit made this rule despite the Supreme Court's admonishment in *Riley v. California* that warrantless searches of electronic devices violate the Constitution via the Fourth Amendment.[34]

The Fourth Amendment would cease to exist at United States borders without the guaranteed protections against unreasonable and warrantless searches and seizures.[35] To alleviate the potential miscarriage of justice embedded in the Eleventh Circuit's standard, the Supreme Court or Congress should require all law enforcement agents at United States borders to identify some level of suspicion before conducting a forensic search of electronic devices.[36] To that end,

---

24. *See* United States v. Molina-Isidoro, 884 F.3d 287, 293 (5th Cir. 2018) (noting only two federal court cases have required reasonable suspicion for a forensic search).

25. United States v. Saboonchi, 990 F. Supp. 2d 536, 548 (D.D.C. 2014).

26. *Id.* at 547.

27. *Id.* at 552.

28. *See* Molina-Isidoro, 884 F.3d at 293 (noting only two federal court cases have required reasonable suspicion for a forensic search).

29. *See* United States v. Cotterman, 709 F.3d 952, 962 (9th Cir. 2013) (en banc) (holding reasonable suspicion is needed to forensically search an electronic device at the border).

30. *See* United States v. Kolsuz, 890 F.3d 133, 141 (4th Cir. 2018) (holding the forensic search of the electronic device at a facility away from the initial stop was constitutional because law enforcement had individualized suspicion).

31. *See* Terry v. Ohio, 392 U.S. 1, 21 (1968) (noting reasonable suspicion arises when an officer can articulate facts that lead him to believe the suspect may be connected to criminal activity).

32. United States v. Touset, 890 F.3d 1227, 1234 (11th Cir. 2018).

33. *Id.*

34. *See* Riley v. California, 573 U.S. 373, 373 (2014) (holding modern cell phones require a high level of protection against unreasonable searches and seizures).

35. U.S. CONST. amend. IV.

36. *Infra* Part IV.

this Comment proceeds as follows.[37] Part II discusses the formation and development of the border search doctrine in the context of the Fourth Amendment.[38] Part III addresses what constitutes a forensic search.[39] Part IV analyzes the leading cases on forensic searches as well as the two Eleventh Circuit cases that created this circuit split.[40] Part V proposes a standard created either by Congress or the Supreme Court that requires law enforcement to have some level of suspicion prior to a forensic search at the border.[41]

II. THE DEVELOPMENT OF UNITED STATES BORDER SEARCHES

The constitutional protection against unreasonable searches and seizures is relaxed at the border, but still in effect.[42] However, the recent precedent from the Eleventh Circuit revoked all previous protections against unreasonable searches and seizures at the border.[43] Section A discusses the laws relating to border searches before the ratification of the Fourth Amendment.[44] Section B addresses the Fourth Amendment's protections against unreasonable searches and seizures.[45] Section C examines the Supreme Court's major decisions on the protections against unconstitutional border searches.[46]

A. Pre-Fourth Amendment Border Protections

The Framers of the United States considered searches at the border reasonable per se before the Fourth Amendment existed.[47] Before Congress ratified the Fourth Amendment, the same Congress passed a customs law allowing for warrantless searches at borders.[48] Specifically, the law "granted customs officials 'full power and authority' to enter and search 'any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed.'"[49] The Supreme Court relied on this legislative history to demonstrate that the drafters of the Fourth Amendment

37. *Infra* Parts II-V.

38. *Infra* Part II.

39. *Infra* Part III.

40. *Infra* Part IV.

41. *Infra* Part V.

42. GOV. PRINTING OFF., FOURTH AMENDMENT: SEARCH AND SEIZURE 1199, 1243 (1992), https://www.gpo.gov/fdsys/pkg/GPO-CONAN-1992/html/GPO-CONAN-1992-10-5.htm (on file with *The University of the Pacific Law Review*).

43. *Infra* Part IV.

44. *Infra* Part II.A.

45. *Infra* Part II.B.

46. *Infra* Part II.C.

47. *See* United States v. Boyd, 116 U.S. 616, 623 (1886) (discussing the Founders' intention to make border searches reasonable per se).

48. GOV. PRINTING OFF., *supra* note 42, at 1200.

49. Act of July 31, 1789, c. 5.1 Stat. 29 § 24.

did not intend for the Fourth Amendment's protections to apply at the border.[50] The Court said "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 (at the border) . . . as unreasonable, and they are not embraced within the prohibition of the amendment."[51] Drawing on the founders, our jurisprudence accepted the notion that border searches are per se constitutional absent a warrant or probable cause well before the establishment of the Fourth Amendment.[52]

B. The Fourth Amendment

The Fourth Amendment protects individuals against unreasonable searches and seizures of one's person, home, papers, and effects.[53] "A search compromises the individual interest in privacy; a seizure deprives the individual of dominion over his or her person or property."[54] A search is unreasonable when it is conducted without a warrant or a legally accepted exception.[55]

The creation of the Fourth Amendment was in direct response to the intrusive searches the American colonists experienced from the British.[56] The British executed unreasonable searches and seizures of colonists without a warrant or with general warrants.[57] In a speech to the British Parliament on general warrants, William Pitt described the need to protect against unreasonable searches and seizures:[58] "The poorest man may in his cottage bid defiance to all the force of the crown. It may be frail—its roof may shake—the wind may blow through it—the storm may enter, the rain may enter—but the King of England cannot enter—all his force dares not cross the threshold of the ruined tenement."[59] The drafters took a cue from Mr. Pitt's warning to Parliament and ratified the Fourth Amendment, ensuring protections against unreasonable searches and seizures.[60]

---

50. United States v. Feiten, No. 15-20631, 2016 WL 894452, at *5 (E.D. Mich. Mar. 9, 2016).

51. *Id.* (quoting United States v. Boyd, 116 U.S. 616, 623 (1886)) (internal quotation marks omitted).

52. United States v. Ramsey, 431 U.S. 607, 616 (1977).

53. U.S. CONST. amend. IV.

54. Horton v. California, 496 U.S. 128, 133 (1990).

55. *See* Katz v. United States, 389 U.S. 347, 357 (1967) ("[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment — subject only to a few specifically established and well-delineated exceptions.").

56. GOV. PRINTING OFF., *supra* note 42, at 1199.

57. *See* United States v. Matlock, 415 U.S. 164, 188 n.1 (1974) (Douglas, J. dissenting) ("Because the Crown had employed the general warrant, rather than the warrantless search, to invade the privacy of the colonists without probable cause and without limitation, it is not surprising that the hatred of the colonists focused on it.").

58. Tracey Maclin, *When the Cure for the Fourth Amendment Is Worse than the Disease*, 68 S. CAL. L. REV. 1, 1 (1994).

59. *Id.*

60. United States v. Weeks, 232 U.S. 383, 390 (1914).

Under the Fourth Amendment, searches or seizures are unreasonable when conducted without a warrant or probable cause.[61] However, there are several exceptions to both the warrant and probable cause requirements.[62] One well-established exception provides that searches and seizures at the border are per se reasonable and do not need a warrant or probable cause.[63]

C. Border Search Cases

Since the ratification of the Fourth Amendment, the Supreme Court has interpreted the Amendment's application to border searches in several landmark cases.[64] Subsection 1 reviews the Court's analysis of physical searches of property at the border in *United States v. Flores-Montano*.[65] Subsection 2 addresses the Court's analysis of searches of individuals at the border in *United States v. Montoya De Hernandez*.[66]

1. United States v. Flores-Montano

In this case, United States Border Patrol agents stopped Mr. Flores-Montano when he tried to enter the United States through a port in Southern California.[67] After the agent instructed Mr. Flores-Montano to get out of his car, the agents transported Mr. Flores-Montano's vehicle to a secondary inspection station.[68] There, agents called a mechanic to inspect the vehicle.[69] Upon arrival, the mechanic, "raised the car on a hydraulic lift, loosened the straps and unscrewed the bolts holding the gas tank to the undercarriage of the vehicle, and then disconnected some hoses and electrical connections."[70] After the mechanic removed the gas tank, he used a chemical substance to open the top of the gas tank to see inside and found contraband.[71]

---

61. Chambers v. Maroney, 399 U.S. 42, 51 (1970).

62. *See* Katz v. United States, 389 U.S. 347, 357 (1967) ("[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment — subject only to a few specifically established and well-delineated exceptions"); Chimel v. California, 395 U.S. 752, 762–63 (1969) (holding that probable cause nor a warrant is required to search an individual or the area within their grabbing range after they have been lawfully arrested); Maryland v. Buie, 494 U.S. 325, 336–37 (1990) (holding that when officers conduct a valid arrest in a home, if there is probable cause to believe harm may be lurking in the home, the officers may do a protective sweep of the home without a warrant).

63. *See* United States v. Ramsey, 431 U.S. 607, 616 (1977) (holding border searches are reasonable because they are conducted at the border).

64. *E.g.*, United States v. Flores-Montano, 541 U.S. 149 (2004); United States v. Montoya De Hernandez, 473 U.S. 531 (1985).

65. *Infra* Section II.C.1.

66. *Infra* Section II.C.2.

67. Flores-Montano, 541 U.S. at 150.

68. *Id.*

69. *Id.* at 151.

70. *Id.*

71. *Id.*

The Court found both the search and the seizure constitutional.[72] According to the Court, Mr. Flores-Montano did not have a privacy interest in his fuel tank, and the agents did not need reasonable suspicion to disassemble his fuel tank.[73] The Court conducted a balancing test of the government's interest in protecting the border and Mr. Flores-Montano's right to privacy.[74] The Court found the government was the clear winner.[75] "The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border."[76] In support of this analysis, the Court quoted *United States v. Ramsey*, "searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border."[77]

The Court's holding expanded the border search doctrine to allow physical manipulation of personal effects.[78] Although agents deconstructed and physically manipulated Mr. Flores-Montano's property, the Court considered it a lawful manual search.[79]

2. United States v. Montoya De Hernandez

In this case, Ms. Montoya De Hernandez flew to Los Angeles, California from Bogota, Colombia, but customs officials did not allow her to enter the United States.[80] A United States customs inspector stopped her because she had made several recent trips to both Los Angeles and Miami.[81] The inspector took her to a second inspection site, questioned her, and led her to a different area for a pat-down and strip search.[82] After the pat down search, officers believed Ms. Montoya De Hernandez was smuggling drugs inside of her body.[83]

After Ms. Montoya De Hernandez refused an x-ray because she asserted she was pregnant, the inspectors gave her three options—leave on the first flight back to Colombia, consent to the x-ray, or remain "in detention until she produced a monitored bowel movement that would confirm or rebut the inspectors' suspicions."[84] Due to issues with her visa, the option to fly back was

72. *Id.* at 155.
73. *Id.* at 152.
74. *Id.*
75. *Id.*
76. *Id.*
77. *Id.* at 152–53 (quoting United States v. Ramsey, 431 U.S. 607, 616 (1977)).
78. *Id.* at 155–56.
79. *Id.*
80. United States v. Montoya De Hernandez, 473 U.S. 531, 533 (1985).
81. *Id.*
82. *Id.* at 534.
83. *Id.*
84. *Id.* at 534–35.

unavailable.[85] Now limited to two options, Ms. Montoya De Hernandez opted to not eat, drink, or use the restroom for sixteen hours.[86] Eventually, a court order forced her to submit to a pregnancy test in order to medically clear her for an x-ray and rectal examination.[87]

The Court held the search and seizure of Ms. Montoya De Hernandez constitutional and the sixteen-hour detention was not unreasonably long.[88] The Court went on to say the search and seizure needed only reasonable suspicion because it occurred at the border and found law enforcement had reasonable suspicion, making the search constitutional.[89]

III. ELECTRONIC SEARCHES

Law enforcement conducts two types of electronic device searches: manual and forensic.[90] At any United States border, law enforcement may manually search an electronic device.[91] Courts consider a manual search of an electronic device a routine search, and therefore, legal.[92] However, any manual search of an electronic device away from the border requires a warrant.[93] Section A discusses the protections the Court developed against warrantless searches of cellphones in *Riley v. California*.[94] Section B outlines routine and a non-routine border search.[95] Section C describes the difference between a manual and a forensic search.[96]

A. Riley v. California

In *Riley*, the Supreme Court refused to extend the search incident to arrest[97] warrant exception to cellphones.[98] Absent specialized exigent circumstances, such as remote wiping, data encryption, or potential physical threats from the

85. *Id.* at 535.

86. *Id.*

87. *Id.*

88. *Id.* at 544.

89. *Id.*

90. United States v. Caballero, 178 F. Supp. 3d 1008, 1016 (S.D. Cal. 2016).

91. *Id.* at 1015.

92. United States v. Kolsuz, 890 F.3d 133, 141 (4th Cir. 2018).

93. *See* Riley v. California, 573 U.S. 373, 388 (2014) (holding absent exigent circumstances, law enforcement needs a warrant to search a cell phone).

94. *Infra* Section III.A.

95. *Infra* Section III.B.

96. *Infra* Section III.C.

97. *See* Chimel v. California, 395 U.S. 752, 762–63 (1969) ("When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape.").

98. Riley v. California, 573 U.S. 373, 373 (2014).

device, a warrant is required to search a cellphone.[99] The Court described why cellphones require such a high level of protection: "[A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is."[100]

The Court listed personal information that may be on a cell phone: medical records, calendars, contacts, messages, addresses, pictures, historic location data, and apps for planning a budget, tracking a pregnancy, improving one's romantic life, and more.[101] The private information a cellphone contains is the type of information the Fourth Amendment tries to protect against unreasonable invasions.[102] In sum, *Riley* highlights the modern understanding that electronic devices present unique privacy issues and deserve additional protections beyond that of any other form of personal property.[103]

B. Routine and Non-Routine Border Searches

Courts across the country agree that law enforcement officers at the border are allowed to conduct routine searches of persons and their effects without reasonable suspicion, probable cause, or a warrant.[104] In order to determine if a search is routine, courts look at the degree of intrusiveness or invasiveness of the search.[105] Courts use the following factors when assessing whether the search was routine:

"(i) whether the search results in the exposure of intimate body parts or requires the suspect to disrobe; (ii) whether physical contact between Customs officials and the suspect occurs during the search; (iii) whether force is used to effect the search; (iv) whether the type of search exposes the suspect to pain or danger; (v) the overall manner in which the search is conducted; and (vi) whether the suspect's reasonable expectations of privacy, if any, are abrogated by the search.[106]

Non-routine searches can intrude deeply into a person's privacy.[107] Recognized types of non-routine searches include strip searches, alimentary-

99. *Id.* at 388–89.

100. *Id.* at 396–97 (emphasis in original).

101. *Id.* at 395–96.

102. *Id.* at 408 (Alito, J., concurring).

103. *See id.* at 373 (holding cellphones may not be searched during a search incident to arrest absent a warrant or exigent circumstances).

104. United States v. Braks, 842 F.2d 509, 511 (1st Cir. 1988).

105. *Id.* at 511.

106. *Id.* at 512.

107. United States v. Kolsuz, 890 F.3d 133, 144 (4th Cir. 2018).

canal searches, and x-rays.[108]

On the other hand, routine searches at the border are exempt from the protections of the Fourth Amendment.[109] Types of routine searches include pat-downs; pocket-dumps; moving or adjusting clothing; scanning, opening, and rifling through the contents of bags or other closed containers; looking inside an automobile gas tank; browsing contents of photograph albums, information encoded on videotapes, or password-protected items; and having a dog sniff at an individual's groin.[110] Courts have also concluded manual searches of electronic devices are considered routine.[111]

C. Manual and Forensic Searches

The search of a computer without any sophisticated forensic techniques and in the same manner that a user would use the computer is a routine and manual search.[112] Therefore, a routine and manual search of an electronic device at the border may be done by law enforcement without any reasonable suspicion.[113]

The techniques used for a forensic search are different from a manual search.[114] A forensic search is more intrusive than a manual search because it goes beyond what a normal user would see on a computer.[115] This is because a forensic search uses "sophisticated technology-assisted search methodologies [that] can exceed vastly the capacity of a human searching and viewing files."[116] A forensic search starts "with the creation of a perfect 'bitstream' copy or 'image' of the original storage device."[117] This bitstream copy is then saved as a read-only file.[118] After that, a computer forensics expert uses specialized software to look at the data.[119] During this process, which can last anywhere from a day to months, the expert reviews all of the contents on the "imaged hard drive, examining the properties of individual files, and probing the drive's unallocated

108. *Id.* at 144.

109. *See id.* at 141 (noting the manual search of Kolsuz's phone was a routine search which are not subject to Fourth Amendment requirements).

110. United States v. Saboonchi, 990 F. Supp. 2d 536, 549 (D.D.C. 2014).

111. *See* Kolsuz, 890 F.3d at 141 (noting the manual search of Kolsuz's phone was a routine search and routine searches are not subject to Fourth Amendment requirements).

112. *Id.* at 144.

113. *See* Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 295 (2015) (noting "[i]n most cases, searches at the border are always permitted even without reasonable suspicion"); *e.g.*, United States v. Arnold, 533 F. 3d 1003, 1008 (9th Cir. 2008) ("[R]easonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border.").

114. Saboonchi, 990 F. Supp. 2d at 547.

115. *Id.*

116. *Id.*

117. *Id.*

118. *Id.*

119. *Id.*

'slack space' to reveal deleted files."[120] The circuit split began when different circuits announced different levels of suspicion required to conduct forensic searches at the border.[121]

IV. CIRCUIT COURT SPLIT ON FORENSIC SEARCHES AT THE BORDER

In 2018, the Eleventh Circuit became the first circuit to hold no level of suspicion is required to forensically search an electronic device at the border.[122] Other circuits have reached the opposite holding.[123] Section A discusses the precedent regarding forensic searches in the Fourth Circuit.[124] Section B examines similar precedent in the Ninth Circuit.[125] Finally, Section C looks at the two Eleventh Circuit cases that eliminated the requirement of any suspicion before forensically searching an electronic device at the border.[126]

A. Fourth Circuit Forensic Border Search Law

The Fourth Circuit held in *United States v. Kolsuz* a forensic search of a digital phone is a non-routine search that requires some level of individualized suspicion.[127] In this case, Mr. Kolsuz had a history of attempting to illegally take firearm parts out of the United States.[128] Before the incident at issue, law enforcement agents stopped Mr. Kolsuz on two previous occasions for having unregistered and unlicensed firearm parts in his suitcase.[129] In both prior instances, Mr. Kolsuz attempted to fly from John F. Kennedy International Airport to Turkey.[130] Both times, law enforcement agents confiscated the illegal firearms parts and instructed Mr. Kolsuz on the law.[131] After these warnings, Mr. Kolsuz again tried to fly out of the United States, this time from Dulles International Airport to Turkey.[132] United States law enforcement found multiple firearms parts in his suitcase, including: eighteen handgun barrels, twenty-two 9mm handgun magazines, four .45 caliber handgun magazines, and other gun

120. *Id.*

121. *Infra* Part IV.

122. United States v. Touset, 890 F.3d 1227, 1234 (11th Cir. 2018).

123. *See* United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013) (en banc) (holding law enforcement must have reasonable suspicion before conducting a forensic search of an electronic device at the border); United States v. Kolsuz, 890 F.3d 133, 144 (4th Cir. 2018) ("forensic border search of a phone must be treated as non-routine, permissible only on a showing of individualized suspicion").

124. *Infra* Section IV.B.

125. *Infra* Section IV.C.

126. *Id.*

127. Kolsuz, 890 F.3d at 146.

128. *Id.* at 138.

129. *Id.*

130. *Id.*

131. *Id.*

132. *Id.* at 139.

components.[133]

The issue before the court was whether the agents' confiscation of Mr. Kolsuz's cellphone and subsequent searches of the cellphone were constitutional.[134] The first search was a manual search, which revealed recent calls and text messages.[135] The court concluded the manual search was a routine search and fell under the border search exception.[136] Thus, the court noted the law enforcement officers did not need reasonable suspicion for the first search.[137]

The court considered the second search a forensic search.[138] The forensic search occurred four miles away from Dulles International Airport at a Homeland Security Investigation office.[139] During this search, a computer forensic agent ran a program on the phone that created an 896-page report of the phone's contents.[140] The report included "personal contact lists, emails, messenger conversations, photographs, videos, calendar, web browsing history, and call logs, along with a history of Kolsuz's physical location down to precise GPS coordinates."[141]

The court held that officers must have individualized suspicion before conducting non-routine forensic searches of electronic devices.[142] Despite the court's lack of a clear standard (e.g., reasonable suspicion), the court noted the agents were correct in this case to rely on the reasonable suspicion standard.[143] The court further noted that despite *Riley*, no precedent requires anything above reasonable suspicion when it comes to forensic searches of electronic devices at the border.[144]

B. Ninth Circuit Forensic Border Search Law

The Ninth Circuit held in *United States v. Cotterman* that there must be a showing of reasonable suspicion before law enforcement can forensically search an electronic device at the border.[145] Subsection 1 discusses the majority opinion in *Cotterman*.[146] Subsection 2 addresses the arguments raised by Judge Callahan's concurrence and Judge Smith's dissent.[147]

---

133. *Id.*
134. *Id.* at 141.
135. *Id.* at 139.
136. *Id.* at 141.
137. *Id.*
138. *Id.*
139. *Id.* at 139.
140. *Id.*
141. *Id.*
142. *Id.* at 146.
143. *Id.* at 148 (Wilkinson, J., concurring).
144. *Id.* at 147 (majority opinion).
145. United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013) (en banc).
146. *Infra* Section IV.B.1.
147. *Infra* Section IV.B.2.

1. Majority Opinion in United States v. Cotterman

In *United States v. Cotterman*, border agents stopped Mr. Cotterman and his wife when the couple tried to enter the United States through Mexico.[148] Mr. Cotterman's previous convictions in 1992 for child molestation and lewd and lascivious conduct triggered an alert at the border crossing.[149] Due to the alert, agents stopped Mr. Cotterman's vehicle.[150] After searching the vehicle, the agents discovered two laptops and a camera.[151] Law enforcement then confiscated the devices and transported them 170 miles away to an Immigration and Customs Enforcement (ICE) office.[152] At the ICE office, a computer forensic examiner used a forensic program to search the electronic devices.[153] During the initial search of the computer, the agent discovered seventy-five images of child pornography.[154]

Later that day, the forensic examiner contacted Mr. Cotterman for assistance in unlocking some password-protected files on Mr. Cotterman's computer.[155] Mr. Cotterman agreed to get back to the forensic examiner once he located the passwords.[156] Instead of supplying the passwords, Mr. Cotterman flew to Mexico the next day and then onward to Australia.[157] Nevertheless, the forensic examiner eventually gained access.[158] The computer had approximately 378 images of child pornography.[159] Most of the images were taken over a two- to three-year period of the same young girl.[160] Several photos depicted Mr. Cotterman sexually molesting a young girl.[161] The forensic examiner continued the search discovering "hundreds more pornographic images, stories, and videos depicting children."[162]

At the first hearing of the case, the Ninth Circuit held reasonable suspicion was not required for this search.[163] However, in an en banc hearing, the court reversed and concluded reasonable suspicion was required for the forensic searches of the electronic devices.[164] Nonetheless, the court determined the

148. Cotterman, 709 F.3d at 957.
149. *Id.*
150. *Id.*
151. *Id.*
152. *Id.* at 958.
153. *Id.*
154. *Id.*
155. *Id.*
156. *Id.*
157. *Id.* at 959.
158. *Id.*
159. *Id.*
160. *Id.*
161. *Id.*
162. *Id.*
163. *Id.*
164. *Id.* at 962.

officers had reasonable suspicion to forensically search Mr. Cotterman's computer and reversed motion to suppress.[165]

2. Concurring and Dissenting Opinions in United States v. Cotterman

In her concurrence, Judge Callahan charged the majority with ignoring over a century of Supreme Court precedent and argued this new rule of requiring reasonable suspicion to forensically search electronic devices is "unworkable and unnecessary, and [would] severely hamstring the government's ability to protect our borders."[166] Judge Callahan made two arguments in her concurrence.[167]

First, a review of the Supreme Court's precedent shows the Court has tried to keep standards for conducting searches at the border flexible.[168] The Court has only required reasonable suspicion in one case.[169] In that case, *Montoya de Hernandez*, the individual was subjected to a 24-hour detention and several intrusive examinations of her person.[170] In all remaining cases before the Supreme Court, the Court confirmed the government's wide authority to search at the border.[171]

Judge Callahan's second argument addressed the three possible border search situations the Court held would not be per se reasonable, and concluded none were applicable in this case.[172] In *Flores-Montano*, the Court announced that a border search might not be reasonable and would require reasonable suspicion in three situations;[173] "highly intrusive searches of the person; destructive searches of property; and conducted in a 'particularly offensive' manner."[174] Judge Callahan indicated the first two situations were plainly not applicable.[175] First, border agents did not search Mr. Cotterman's person—just his property.[176] Second, the border agents did not destroy Mr. Cotterman's property.[177] As for the third justification, Judge Callahan argued searching a computer, which is capable of storing a large amount of personal information, does not make the search "particularly offensive."[178] For support, Judge Callahan cited Ninth Circuit precedent stating searching computers does not enhance Fourth Amendment

165. *Id.* at 970.
166. *Id.* at 971 (Callahan, J., concurring).
167. *Id.*
168. *Id.* at 971–72.
169. *Id.* at 971.
170. *Id.* at 971–72 (citing United States v. Montoya De Hernandez, 473 U.S. 531, 541 (1985)).
171. *Id.* at 972.
172. *Id.* at 973.
173. *Id.*
174. *Id.*
175. *Id.* at 974–75.
176. *Id.* at 973.
177. *Id.*
178. *Id.* at 977.

protections.[179] "[C]omputers are [not] special for Fourth Amendment purposes by virtue of how much information they store; neither the quantity of information, nor the form in which it is stored, is legally relevant in the Fourth Amendment context."[180]

In his dissent, Judge Smith voiced a policy concern stating the majority's ruling would burden law enforcement and create national security issues.[181] The dissent said law enforcement would have to make a "complex legal determination on the spot."[182] Under the standard created by the majority, law enforcement must determine if a search of an individual's data is allowed because it is "unintrusive" or if the search is illegal because it is "comprehensive and intrusive."[183] The dissent notes a Customs and Border Protection directive, "border searches of electronic storage devices are 'essential' for 'detect[ing] evidence relating to terrorism and other national security matters.'"[184] Echoes of Judge Callahan's and Judge Smith's arguments are present in the two 2018 Eleventh Circuit cases adopting suspicion-less forensic searches at the border.[185]

C. Eleventh Circuit Forensic Border Search Law

The Eleventh Circuit recently announced new precedent on the constitutionality of searches of electronic devices at the border.[186] Subsection 1 reviews the Eleventh Circuit holding in *United States v. Vergara*.[187] In that case, the court rejected requiring a warrant or probable cause to forensically search electronic devices at the border.[188] Subsection 2 analyzes the Eleventh Circuit case of *United States v. Touset*.[189] *Touset* created the circuit split when the court announced law enforcement does not need any suspicion to forensically search an electronic device at the border.[190]

---

179. *Id.* at 978.

180. *Id.* (quoting United States v. Giberson, 527 F.3d 882, 888 (9th Cir. 2008)).

181. *Id.* at 984 (Smith, J., dissenting).

182. *Id.*

183. *Id.*

184. *Id.* at 985 (alteration in original).

185. *See* United States v. Touset, 890 F.3d 1227, 1229 (11th Cir. 2018) (holding the Fourth Amendment does not require any suspicion for forensic searches of electronic devices at the border); United States v. Vergara, 884 F.3d 1309, 1312 (11th Cir. 2018) (holding border searches never require probable cause or a warrant and only highly intrusive border searches require reasonable suspicion).

186. Touset, 890 F.3d at 1229 (holding the Fourth Amendment does not require any suspicion for forensic searches of electronic devices at the border); Vergara, 884 F.3d at 1309 (holding border searches never require probable cause or a warrant and only highly intrusive border searches require reasonable suspicion).

187. *Infra* Section IV.C.1.

188. *Infra* Section IV.C.1.

189. *Infra* Section IV.C.2.

190. *Infra* Section IV.C.2.

1. United States v. Vergara

In *Vergara*, the Eleventh Circuit held border searches never require a warrant or probable cause.[191] Mr. Vergara returned to Florida on a cruise ship from Mexico.[192] Officers stopped and searched Mr. Vergara because of his prior conviction for possession of child pornography.[193] During the search, officers found three cellphones in Mr. Vergara's possession.[194] During a manual search of one phone, the officer immediately recognized a video as possible child pornography.[195] The officer reached out to a criminal investigator with the Department of Homeland Security who confirmed the video was child erotica.[196] After this discovery, a Homeland Security officer confiscated the cellphones in order to conduct forensic searches on them.[197] The search uncovered "more than 100 images and videos of child pornography and erotica stored on Vergara's phones."[198]

After reviewing the facts in this case, the court reaffirmed the law that searches at the border do not require a warrant or probable cause.[199] However, the court noted reasonable suspicion might be required in cases of "highly intrusive searches of a person's body such as a strip search or an x-ray examination."[200]

The court implied searches of electronic devices, whether manual or forensic, would not require a warrant or probable cause.[201] The court avoided the issue of whether reasonable suspicion is required when forensically searching electronic devices at the border because Mr. Vergara did not challenge the lack of reasonable suspicion.[202] Additionally, the court said only certain searches of a person require reasonable suspicion, but reasonable suspicion is not required for searches of property.[203]

Two months later, the same court in an opinion by the same judge held suspicion-less forensic searches of electronic devices at the border are constitutional.[204]

---

191. Vergara, 884 F.3d at 1312.

192. *Id.* at 1311.

193. *Id.*

194. *Id.*

195. *Id.*

196. *Id.* at 1314 (Pryor, J., dissenting).

197. *Id.*

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

199. *Id.* at 1312.

200. *Id.*

201. *Id.*

202. *Id.* at 1313.

203. *Id.* at 1312 (holding border searches do not require a warrant or probable and that only highly intrusive searches of a person require reasonable suspicion).

204. *See* United States v. Touset, 890 F.3d 1227, 1229 (11th Cir. 2018) (holding the Fourth Amendment does not require any suspicion for forensic searches of electronic devices at the border).

2. United States v. Touset

Judge Pryor, of the Eleventh Circuit, expanded the rule from *Vergara* by announcing in *Touset* that no suspicion is required to forensically search an electronic device at the border.[205] In this case, the investigation of Mr. Touset started long before he arrived at Hartsfield-Jackson Atlanta International Airport.[206]

Xoom, a company that transmits money, noticed a pattern of transfers consistent with "people it suspected were involved with child pornography."[207] Xoom learned that Mr. Touset's account was linked with Yahoo email and messenger accounts.[208] With that information, Xoom contacted both Yahoo and the National Center for Missing and Exploited Children.[209] During an investigation, Yahoo found the account Xoom identified.[210] The account had a file containing child pornography.[211] Yahoo sent this information to the National Center for Missing and Exploited Children, which in turn notified the Cyber Crime Center of the Department of Homeland Security.[212]

After the Department of Homeland Security issued subpoenas in relation to the investigation, Western Union responded with Mr. Touset's name and post office box, which was also linked to the Yahoo account.[213] All of this investigation occurred before Mr. Touset's international flight even touched down in Atlanta, Georgia.[214]

Once Mr. Touset arrived, an officer from Customs and Border Protection searched his luggage and discovered several electronic devices: two iPhones, a camera, two laptops, two external hard drives, and two tablets.[215] Law enforcement confiscated and conducted a forensic search on the devices revealing child pornography on the laptops and the external hard drives.[216] With this evidence, law enforcement secured a warrant to search Mr. Touset's home in Georgia.[217] The search turned up evidence of thousands of images of child pornography and uncovered Mr. Touset paid over $55,000 for "pornographic pictures, videos, and webcam sessions" and an "excel spreadsheet that documented the names, ages, and birthdates of young girls in the photos, as well

205. *Id.*
206. *Id.* at 1230.
207. *Id.*
208. *Id.*
209. *Id.*
210. *Id.*
211. *Id.*
212. *Id.*
213. *Id.*
214. *Id.*
215. *Id.*
216. *Id.*
217. *Id.*

as his personal notes about them."[218]

The court held reasonable suspicion was not required to forensically search the electronic devices because the search was of property and not a person.[219] The court openly acknowledged conducting an intrusive search of a person at the border requires reasonable suspicion.[220] Further, the court conceded a search of an electronic device may be intrusive;[221] however, the court stood by its interpretation of the jurisprudence and held, "our precedents do not require suspicion for [an] intrusive search of any property at the border."[222]

Mr. Touset argued the Supreme Court's ruling in *Riley* was meant to protect privacy by requiring a warrant to search all cellphones.[223] The court in *Touset* disagreed and reiterated the holding in *Riley* is limited to the search incident to arrest exception, which was not applicable with this case.[224] Therefore, the court resorted to the border search doctrine for guidance.[225]

The court reiterated the need for a balance between the government's security interest and an individual's privacy interest.[226] The Ninth Circuit and the Fourth Circuit in *Cotterman* and *Kolsuz* argued travelers could not protect their privacy because it is impractical and unreasonable for travelers to travel without their electronic devices.[227] In contrast, the *Touset* court asserted travel has been inconvenient for quite some time and travelers grow accustomed to inconveniences.[228] The court mentioned some inconvenience of modern travel such as "screening procedures that require passengers to unpack electronic devices, separate and limit liquids, gels, and creams, remove their shoes, and walk through a full-body scanner."[229] The court emphasized property, unlike persons, could always be left at home when traveling and remain free from searches.[230]

After allowing suspicion-less forensic searches at borders, the court said, "if we were to require reasonable suspicion for searches of electronic devices, we would create special protections for the property most often used to store and

---

218. *Id.* at 1230–31.

219. *See id.* at 1234 (noting "property and persons are different").

220. *Id.*

221. *Cf.* United States v. Cotterman, 709 F.3d 952, 977 (9th Cir. 2013) (en banc) (Callahan, J., dissenting) (arguing searching a computer is not particularly offensive).

222. Touset, 890 F.3d at 1234 (citing United States v. Alfaro-Moncada, 607 F.3d 720, 728–29, 732 (11th Cir. 2009)).

223. *Id.*

224. *Id.*

225. *Id.*

226. *Id.* at 1236.

227. United States v. Cotterman, 709 F.3d 952, 965 (9th Cir. 2013) (en banc); United States v. Kolsuz, 890 F.3d 133, 145 (4th Cir. 2018).

228. Touset, 890 F.3d at 1235.

229. *Id.* (citing Corbett v. Transp. Sec. Admin., 767 F.3d 1171, 1174 (11th Cir. 2014)).

230. *Id.*

disseminate child pornography."[231] In the opinion, the court called upon Congress to make a law dictating the standard required for a forensic search of electronic devices at the border.[232] "Instead of 'charging unnecessarily ahead,' we must allow Congress to design the appropriate standard 'through the more adaptable legislative process and the wider lens of legislative hearings.'"[233]

In order to insulate the case from Supreme Court review, Judge Pryor wrote the opinion in a manner limiting the Supreme Court's ability to hear the case.[234] The court in *Touset* held that even if reasonable suspicion was required in order for the search to be constitutional, law enforcement had reasonable suspicion for the search.[235] By holding the search constitutional, the Supreme Court would not be able to change the outcome of this case, making the case nonjusticiable.[236] The Supreme Court could only change the law, not the outcome, which likely lessened the chance of Supreme Court review.[237]

V. POLICY CONSIDERATIONS

Supporters of the Eleventh Circuit's holding in *Touset* fail to look past the limited reasoning the court supplies.[238] In *Touset*, the court feared there was no feasible way to protect against child pornography entering the country.[239] While the court's concern might be valid, it is also shortsighted.[240] Officials might stop and search under the guise of protecting against child pornography, but how would a traveler know that was the *actual* reason for the search?[241] There is no legal requirement for officers to explain the reason for a stop and search.[242] The search could be motivated by any discriminatory basis, including gender, political affiliation, religion, nationality, age, disability, or worse, no reason at all.[243]

---

231. *Id.*

232. *Id.* at 1237.

233. *Id.* (citing United States v. Kolsuz, 890 F.3d 133, 150 (4th Cir. 2018) (Wilkinson, J., concurring)).

234. Kerr, *supra* note 113.

235. Touset, 890 F.3d at 1233.

236. Kerr, *supra* note 113.

237. *Id.*

238. *See generally Forensic Searches of Digital Information at the Border – Eleventh Circuit Holds that Border Searches of Property Require No Suspicion*, 132 HARV. L. REV. 1112 (2019) [hereinafter *Forensic Searches*] (agreeing with the Eleventh Circuit reasoning that preventing child pornography from entering the country was a sufficient basis for allowing suspicionless forensic searches of electronic devices at the border).

239. Touset, 890 F.3d at 1236.

240. *Forensic Searches*, *supra* note 238, at 1119.

241. *See* Brief of the American Civil Liberties Union, ACLU of Illinois, and the Electronic Frontier Foundation as Amici Curiae Supporting Defendant-Appellant at 9, United States v. Wanjiku, No. 18-1973 (7th Cir. argued Nov. 7, 2018), 2018 WL 3602348, at *9 ("To rule otherwise would give the government unfettered access to an incredible compendium of the most intimate aspects of people's lives simply because they have decided to travel internationally.").

242. Touset, 890 F.3d at 1233.

243. *Cf. id.* (holding no suspicion is required to forensically search an electronic device at the border).

This "parade of horribles" could very easily turn into a reality.[244] Under the Eleventh Circuit's precedent, any forensic search of electronic devices at the border is reasonable per se.[245] Any traveler through any point of entry into the United States in the Eleventh Circuit's jurisdiction could have every electronic device taken, copied, and forensically examined without cause.[246] The Fourth Amendment is still in the Constitution, despite the Eleventh Circuit's holding in *Touset*.[247]

Not only is allowing law enforcement free range to forensically search any electronic device unconstitutional under the Fourth Amendment, it implicates other fundamental rights, namely, privacy.[248] Consider the following hypotheticals: honeymooners return home with private photos, a CEO of a foreign entity has confidential strategic plans on her laptop, a doctor with patient information in his email, an attorney with confidential client information on her hard drive—all information the United States government can view, copy, and study without cause.[249]

VI. RECOMMENDATIONS

To resolve the circuit split and maintain the Fourth Amendment's protections, Congress should act to ensure forensic searches of electronics at the border require reasonable suspicion.[250] In lieu of a Congressional rule, Section A addresses a possible Supreme Court solution.[251] Section B discusses the more pragmatic solution of a law created by Congress.[252]

A. Supreme Court Solution

In order to protect Fourth Amendment rights, the Supreme Court should review a case concerning forensic searches at the border.[253] To preserve the

244. Ben Zimmer, *Where Did the Supreme Court Get 'Its Parade of Horribles'?: How an Obscure Fourth of July Custom from New England Spawned a Legal-World Insult*, BOSTON GLOBE (July 1, 2012), https://www.bostonglobe.com/ideas/2012/06/30/where-did-supreme-court-get-its-parade-horribles/Y0jnIscamtgPEzO0PdtL9N/story.html (on file with *The University of the Pacific Law Review*).

245. Touset, 890 F.3d at 1233.

246. *See id.* (holding no suspicion is required to forensically search an electronic device at the border).

247. U.S. CONST. amend. IV; *see also* Touset, 890 F.3d at 1234 (holding forensic searches of electronic devices at the border require no level of suspicion).

248. *See* Novak, *supra* note 1 (recounting stories of Customs and Border Patrol taking individual's phones and searching them).

249. *See id.* (recounting stories of Customs and Border Patrol taking individual's phones and searching them).

250. *Infra* Part VI.

251. *Infra* Section VI.A.

252. *Infra* Section VI.A.

253. *See* Kerr, *supra* note 113 (noting the Supreme Court will likely not take up United States v. Touset because the Court would not be able to change the outcome of the case, only the law).

Fourth Amendment and adhere to precedent, the Court should require reasonable suspicion before conducting a forensic search of electronic devices at the border.[254] This would allow the Court to engage in a balance testing between the government interest in protecting the border and preserving individual rights.[255] Such a ruling would follow the reasoning in *Riley* by recognizing electronic devices are different than other types of personal property and deserve special protections due to the privacy risks presented.[256] This ruling would also maintain the government's strong interest in securing the border by continuing to allow manual searches of electronic devices.[257]

However, a judicial holding would allow the Court to create a standard on a matter that is typically reserved to Congress.[258] "Imposing a Fourth Amendment floor at the border without congressional input would amount to an inflexible, 'hugely consequential policy judgment' that would lack the benefits of consultation with national security officials and privacy advocacy groups, as well as the constraining influence of legislative consensus-building."[259]

Further, courts have already tried to grapple with the complex balancing test and refused to make a decision due to the complicated issues.[260] In the Northern District of Illinois, Judge Bucklo refused to answer whether a forensic preview is a non-routine search requiring reasonable suspicion.[261] Judge Bucklo fought between siding with the Court's reasoning in *Riley* and the reasoning in *Montoya de Hernandez*.[262] Unable to see a clear victor in this balancing test, Judge Bucklo denied the motion to suppress the evidence on the grounds that the officers had at least reasonable suspicion for the search.[263]

B. A Congressional Solution

In lieu of a Supreme Court ruling, Congress should pass a statute to resolve the circuit split by requiring reasonable suspicion in order to conduct a forensic

254. *See* United States v. Cotterman, 709 F.3d 952, 968 (9th Cir. 2013) (en banc) (holding forensic searches of electronic devices at the border require reasonable suspicion).

255. *See* United States v. Flores-Montano, 541 U.S. 149, 152 (2004) (engaging in a balancing test between the government's interest in protecting the border and individual privacy interest).

256. *See* Riley v. California, 573 U.S. 373, 401–02 (2014) (holding the search incident to arrest exception does not apply to electronic devices absent exigent circumstances).

257. *See* United States v. Touset, 890 F.3d 1227, 1237 (11th Cir. 2018) (the court called for the legislative branch to make a law deciding the standard needed to forensically search electronic devices at the border).

258. *Forensic Searches*, *supra* note 238, at 1119.

259. *Id.* (quoting United States v. Kolsuz, 890 F.3d 133, 151 (4th Cir. 2018)).

260. United States v. Wanjiku, No. 16 CR 296, 2017 WL 1304087, at *5 (N.D. Ill. Apr. 6, 2017).

261. *Id.* ("I conclude that this is not the appropriate case in which to wrestle these difficult issues to the ground.").

262. *Id.*

263. *Id.*

search of an electronic device at the border.[264] A statute may be preferable to a Supreme Court ruling because it would allow for full discussion of the issue with stakeholders through the legislative process.[265] This statutory solution could promote stability and clarity by defining forensic searches and providing that only certain electronic devices, such as cellphones and laptops, deserve this increased protection.[266] Despite Judge Callahan's concern that having law enforcement engage in a reasonable suspicion test is unnecessarily burdensome, the United States Customs and Border Protection has issued a directive requiring reasonable suspicion for a forensic search.[267] This directive shows a statute requiring reasonable suspicion is feasible and not overly burdensome.[268] Through a statutory solution, Congress can ensure the Fourth Amendment continues to protect privacy, even at the border.[269]

VIII. CONCLUSION

In May 2018, a circuit split emerged putting the Eleventh Circuit at odds with the Ninth and Fourth Circuits.[270] The Eleventh Circuit held reasonable suspicion is not required to conduct a forensic search of electronic devices at the border.[271] In contrast, the Ninth and Fourth Circuits held that either reasonable suspicion or some level of individualized suspicion is required in order to conduct this type of search.[272] Despite the strong legislative intent and historical background on the protections afforded in the Fourth Amendment, the Eleventh Circuit relied primarily on the border search doctrine for support in reaching its conclusion.[273] The other two circuits relied on the Fourth Amendment for support in requiring some level of suspicion.[274]

To resolve this circuit split, the Supreme Court or Congress should set out a standard governing the level of suspicion required at the border to create uniformity throughout all of the United States' borders.[275] Reasonable suspicion

264. *See, e.g.*, Traveler's Privacy Protection Act of 2008, S. 3612, 110th Cong. § 4 (proposing to require reasonable suspicion before an electronic device could be searched at the border).

265. *See The Legislative Process*, UNITED STATES HOUSE OF REPRESENTATIVES, https://www.house.gov/the-house-explained/the-legislative-process (last visited Jan. 12, 2019) (on file with *The University of the Pacific Law Review*).

266. *See* Traveler's Privacy Protection Act of 2008, S. 3612, 110th Cong. § 3 (providing definitions for the bill, such as "electronic equipment").

267. Kevin McAleenan, U.S. Customs and Border Patrol, Directive No. 3340-049A, at 5 (Jan. 4, 2018).

268. *See id.* (requiring reasonable suspicion before an "advanced search" may be conducted).

269. *See, e.g.*, Traveler's Privacy Protection Act of 2008, S. 3612, 110th Cong. § 4 (proposing to require reasonable suspicion before an electronic device could be searched at the border).

270. *Supra* Part I.

271. *Supra* Part I.

272. *Supra* Part I.

273. *Supra* Part II.

274. *Supra* Part IV.

275. *Supra* Part VI.

should be the standard to conduct a forensic search of an electronic device at the border.[276] The clear language of the Fourth Amendment against unreasonable searches and seizures, as well as the Supreme Court's recent holding in *Riley*, indicate the constitutional right against unreasonable searches and seizures encompasses electronic devices, even if searched at the border.[277]

276. *Supra* Part VI.

277. *Supra* Part VI.