BORDER SEARCHES OF ELECTRONIC DEVICES

INTRODUCTION

In fiscal year 2018, U.S. Customs and Border Protection ("CBP") searched 33,295 electronic devices at the border without first needing a warrant.[1] In fiscal year 2015, only about 8,500 electronic devices were searched at the border; in fiscal year 2016 that number rose to about 19,000; in fiscal year 2017 the number of devices searched increased again to over 30,000.[2] The continued nontrivial increases in the number of electronic devices searched at the border, amounting to over 33,000 in fiscal year 2018, reveal that border searches of electronic devices are occurring more and more frequently with each passing year. The government is able to conduct these searches without obtaining warrants because, while the Fourth Amendment protects individuals' "persons, houses, papers, and effects" from unreasonable searches and seizures,[3] searches at the border have been exempt from Fourth Amendment protection. This exception is known doctrinally as the border search exception.[4] The border search exception originally was designed to allow border agents to search travelers' luggage for contraband and other harmful materials.[5] However, with the progress of technology, the border search exception is now being exploited by border agents to conduct forensic searches of travelers' electronic devices.[6] Forensic searches are essentially "computer strip search[es],"[7] wherein the government uses forensic software to access all active or readable files on the device, as well as password-protected data, hidden or encrypted data,

1. Joint Statement of Stipulated Facts, Ex. 46 ¶ 13, Alasaad v. Nielsen, No. 17-cv-11730-DJC (D. Mass. Apr. 30, 2019). The stipulations in the *Alasaad* case lists the number of border searches of electronic devices for the past seven years, with 33,295 devices searched in fiscal year 2018 marking a sizable increase from the 30,524 in fiscal year 2017. *Id.* A press release from the CBP reported a lower number of 30,200 border searches of electronic devices for fiscal year 2017. Press Release, U.S. Customs & Border Prot., CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics (Jan. 5, 2018), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and [https://perma.cc/3HS9-SUSJ].

2. 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/ [https://perma.cc/W9VC-67F8].

3. U.S. CONST. amend. IV ("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.").

4. United States v. Ramsey, 431 U.S. 606, 621 (1977) ("[T]he 'border search' exception . . . . is a longstanding, historically recognized exception to the Fourth Amendment's general principle that a warrant be obtained . . . .").

5. *Id.* at 618.

6. *See supra* note 1 and accompanying text.

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

deleted files, metadata, and unallocated file space.[8] The smartphones, laptops, and tablets which accompany travelers to the border provide border agents unfettered access to vast quantities of personal information, without the protection of the Fourth Amendment.[9]

The Supreme Court has not ruled on how to treat forensic searches of electronic devices at the border, leaving circuit courts to grapple with the question.[10] The Eleventh Circuit held that the border search exception squarely applies to electronic devices, awarding no more privacy protections to smartphones or laptops than is given to suitcases and backpacks at the border.[11] The Fourth and Ninth Circuits held that the privacy interests implicated in electronic devices outweigh the governmental interests in border security, therefore border agents must possess "reasonable suspicion" of criminal activity before conducting a forensic search of an electronic device.[12] No circuit court has held that border agents need a warrant to forensically search an electronic device. The splintering among circuits is caused by the collision of two important policy interests, privacy rights and border security, leaving the law in chaos.[13]

While the Supreme Court has not weighed in on the treatment of electronic devices at the border, in recent cases that did *not* take place at the border, the Supreme Court has carved out protections in Fourth Amendment doctrine for searches of digital data. These cases offer guidance as to how the privacy interests in digital data and electronic devices should be understood when balanced against the governmental interests at the border.[14]

This Note first provides background on the Fourth Amendment and the border search exception. Second, this Note discusses the landmark cases

8. *See* NAT'L INST. OF JUSTICE, U.S. DEP'T OF JUSTICE, FORENSIC EXAMINATION OF DIGITAL EVIDENCE: A GUIDE FOR LAW ENFORCEMENT 16 (2004) [hereinafter NIJ FORENSIC EXAMINATION GUIDE], https://www.ncjrs.gov/pdffiles1/nij/199408.pdf [https://perma.cc/25YF-C47P].

9. *Id.*

10. The Eleventh Circuit and the Fourth and Ninth Circuits are split as to how forensic searches of electronic devices should be treated at the border. *Compare* United States v. Touset, 890 F.3d 1227, 1229 (11th Cir. 2018) (holding that the border search exception applies to electronic devices just as it would to other property brought to the border), *with* United States v. Kolsuz, 890 F.3d 133, 144 (4th Cir. 2018) (holding that electronic devices are categorically different from other objects and therefore the border search exception should be narrowed to require some level of reasonable or individualized suspicion to forensically search them at the border), *and Cotterman*, 709 F.3d at 968 (holding the same).

11. *Touset*, 890 F.3d at 1229.

12. *Kolsuz*, 890 F.3d at 144; *Cotterman*, 709 F.3d at 968.

13. *See Touset*, 890 F.3d at 1229; *Kolsuz*, 890 F.3d at 144; *Cotterman*, 709 F.3d at 968.

14. *See* Riley v. California, 573 U.S. 373, 386 (2014) (holding that a warrant is required to search a cell phone even if the phone is seized incident to an arrest, thereby deviating from the established incident to arrest exception to the warrant requirement); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018) (holding that a warrant is required to search the record a cell phone creates of its user's movements, even though the user's location information was shared with a third party, thereby deviating from the established third-party doctrine exception to the warrant requirement).

Riley v. California and *Carpenter v. United States* to demonstrate how the Supreme Court has addressed digital data in the Fourth Amendment context. Third, this Note examines the circuit split between the Eleventh Circuit and the Fourth and Ninth Circuits regarding how electronic devices have been treated at the border. This Note then assesses the arguments for and against warrantless forensic searches of electronic devices at the border, and resolves the legal conflict in favor of greater privacy protections in electronic devices at the border.

Because searches of electronic devices implicate serious privacy interests, because travelers cannot mitigate the risk to their privacy at the border, and because a higher standard does not significantly hinder the governmental interests present at the border, border agents should be required to obtain a warrant before searching electronic devices. Short of a warrant, border agents, at a minimum, should be required to possess reasonable suspicion before searching electronic devices.

I. THE BORDER SEARCH EXCEPTION TO THE FOURTH AMENDMENT

The Fourth Amendment protects "persons, houses, papers, and effects" from unreasonable searches and seizures.[15] To conduct a search or seizure within the scope of Fourth Amendment protection, the government must first show probable cause and obtain a warrant.[16] The purpose of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."[17]

At the same time, the Supreme Court has recognized a longstanding exception to the Fourth Amendment for searches conducted at the border.[18] The border search exception originates from the "longstanding right of the sovereign to protect itself" from harm caused by people and property crossing the border.[19] The exception stems from the governmental interest in preventing "unwanted persons and effects,"[20] including contraband, communicable disease, narcotics, explosives, and other threats to national security, from crossing the border.[21] Nevertheless, even at the border, courts have rejected an "anything goes" approach.[22] The Supreme Court has distinguished between two types of searches—routine and nonroutine—

15. U.S. CONST. amend. IV.
16. *Id.*
17. *Carpenter*, 138 S. Ct. at 2213 (quoting Camara v. Mun. Court of City & Cty. of S.F., 387 U.S. 523, 528 (1967)).
18. United States v. Ramsey, 431 U.S. 606, 621 (1977).
19. *Id.* at 616.
20. United States v. Flores-Montano, 541 U.S. 149, 152 (2004).
21. United States v. Montoya de Hernandez, 473 U.S. 531, 537–39, 544 (1985).
22. United States v. Seljan, 547 F.3d 993, 1000 (9th Cir. 2008).

which places limits on border agents' ability to conduct searches in certain circumstances.[23]

For routine searches at the border, border agents do not need any reason to search persons and property entering or exiting the country.[24] Routine searches at the border are considered per se reasonable.[25] The governmental interests at the border, such as national security and the sovereign's interest in preventing contraband from entering the country, make routine searches reasonable by virtue of being at the border.[26] Examples of routine searches include straightforward searches such as looking in "suitcases, wallets, purses, or overcoats,"[27] as well as more involved searches such as disassembling a vehicle's gas tank,[28] pat down searches,[29] close-up sniffing by a trained narcotics-detection dog,[30] x-raying and drilling holes in luggage,[31] looking through photo albums or video tapes,[32] and even manual (non-forensic) reviews of cell phone or computer contents.[33]

In contrast to routine searches, nonroutine searches require that border agents meet a higher standard of reasonableness, thereby narrowing the border search exception.[34] Nonroutine border searches are only reasonable if they are based on "reasonable suspicion."[35] The Supreme Court has identified three types of nonroutine searches: "highly intrusive searches of the person," destructive searches of property, and searches conducted in a "particularly offensive" or overly intrusive manner.[36] In practice, nonroutine searches consist of searches such as "strip searches, body cavity searches, searches that destroy property, and prolonged detentions of

23. *Montoya de Hernandez*, 473 U.S. at 541 & n.4.
24. *Id.* at 538.
25. *Id.*
26. *Id.* at 537–38; *see also* United States v. Ramsey, 431 U.S. 606, 616 (1977) ("That searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border, should, by now, require no extended demonstration.").
27. Jared Janes, *The Border Search Doctrine in the Digital Age: Implications of* Riley v. California *on Border Law Enforcement's Authority for Warrantless Searches of Electronic Devices*, 35 REV. LITIG. 71, 75–78 (2016).
28. United States v. Flores-Montano, 541 U.S. 149, 155–56 (2004).
29. United States v. Beras, 183 F.3d 22, 26 (1st Cir. 1999).
30. United States v. Kelly, 302 F.3d 291, 294 (5th Cir. 2002).
31. United States v. Lawson, 461 F.3d 697, 701 (6th Cir. 2006).
32. United States v. Saboonchi, 990 F. Supp. 2d 536, 549 (D. Md. 2014) (citing United States v. Ickes, 393 F.3d 501, 502–03 (4th Cir. 2005)).
33. *See, e.g.*, United States v. Stewart, 729 F.3d 517, 521, 525 (6th Cir. 2013) (holding a "non-forensic examination" of a computer involving scrolling through images was a "routine border search"); United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008) (holding that a search by a border agent which involved turning on a laptop and viewing files was reasonable per se).
34. Janes, *supra* note 27, at 76–77.
35. *Id.* at 77.
36. United States v. Flores-Montano, 541 U.S. 149, 152–56, 154 n.2 (2004).

individuals."[37] It is within the third category, overly intrusive searches, that some courts have found forensic searches of electronic devices to be nonroutine.[38]

The Supreme Court defines reasonable suspicion as "a particularized and objective basis for suspecting the particular person stopped of criminal activity" determined in light of the "totality of the circumstances."[39] The law measures intrusiveness by how deeply a search implicates a person's privacy and dignity interests.[40] Yet, the Supreme Court has not articulated a clear test for what makes a border search reasonable or unreasonable, and instead employs a case-by-case analysis.[41] Nevertheless, the fact that the Supreme Court acknowledges that certain searches at the border require an objective basis of reasonableness demonstrates that the law could develop to pay heed to the privacy interests of the digital age.

II. THE SUPREME COURT'S TREATMENT OF SEARCHES INVOLVING DIGITAL DATA

In cases away from the border, the Supreme Court has confronted how searching electronic devices maps onto existing Fourth Amendment doctrine. Understanding how the Supreme Court treats searches of electronic devices away from the border provides guidance as to how they should be treated at the border.

A. Riley v. California

The landmark case *Riley v. California* significantly influenced the treatment of cell phones and electronic devices in Fourth Amendment doctrine.[42] *Riley* involved a warrantless search of data stored on a cell phone when the phone was found on the defendant at the time of arrest.[43] The lower court held that searching the defendant's phone without a warrant was reasonable because it was a search incident to an arrest, which places the

37. Janes, *supra* note 27, at 77; *see also* United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985) (holding a nonroutine border search is justified if border agents have reasonable suspicion that the traveler was engaged in smuggling contraband in her alimentary canal).

38. *See* United States v. Kolsuz, 890 F.3d 133, 144–46 (4th Cir. 2018); United States v. Cotterman, 709 F.3d 952, 963, 967–68 (9th Cir. 2013).

39. United States v. Cortez, 449 U.S. 411, 417–18 (1981).

40. *Kolsuz*, 890 F.3d at 138.

41. *Cotterman*, 709 F.3d at 963.

42. *See generally* Janes, *supra* note 27 (discussing the impact of *Riley* on Fourth Amendment Doctrine in the border context); Eunice Park, *The Elephant in the Room: What Is a "Nonroutine" Border Search, Anyway? Digital Device Searches Post*-Riley, 44 HASTINGS CONST. L.Q. 277 (2017) (same); Thomas Mann Miller, Comment, *Digital Border Searches After* Riley v. California, 90 WASH. L. REV. 1943 (2015) (same).

43. Riley v. California, 573 U.S. 373, 378 (2014).

search within the purview of the incident to arrest exception to the Fourth Amendment.[44] The policy reason for this exception stems from the governmental interests in protecting officers' safety (in case the individual arrested has weapons on his person) and in preventing the destruction of evidence (in case the arrested individual tries to destroy evidence on his person).[45]

However, the Supreme Court unanimously reversed, holding that a warrantless search of a cell phone searched incident to an arrest is unconstitutional because the policy reasons which gave rise to the incident to arrest exception are not present when the search is of a cell phone or consists of digital data.[46]

Furthermore, the Court articulated that searching cell phones is categorically different in both "a quantitative and a qualitative sense"[47] from more traditional searches. Cell phones are quantitatively different because they allow large quantities of personal information to be held "literally in the hands of individuals."[48] The immense storage capacity of cell phones exposes vast amounts of private information if searched, whereas more traditional objects would implicate a lesser amount of private information.[49]

Additionally, cell phones are qualitatively different because of the sensitive nature of the information they hold and the universality of cell phone use.[50] "Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day."[51] Cell phones collect various types of information like addresses, prescriptions, bank statements, and videos.[52] Information on cell phones can be used to reconstruct a person's private life and serve as a record dating back to the purchase of the cell phone, or earlier, that can be searched and sifted through; information contained in traditional objects found on a

44. *Id.* at 380.

45. *Id.* at 384–85 ("[C]oncerns for officer safety and evidence preservation underlie the search incident to arrest exception."); *see also* Arizona v. Gant, 556 U.S. 332, 338 (2009) ("The [incident to arrest] exception derives from interests in officer safety and evidence preservation that are typically implicated in arrest situations."); United States v. Robinson, 414 U.S. 218, 228–29 (1973) (noting the policy justifications for the incident to arrest exception include concern for officer safety and evidence preservation).

46. *Riley*, 573 U.S. at 386 ("*Robinson* concluded that the two risks . . . —harm to officers and destruction of evidence—are present in all custodial arrests. There are no comparable risks when the search is of digital data. . . . We therefore decline to extend *Robinson* to searches of data on cell phones, and hold instead that officers must generally secure a warrant before conducting such a search.").

47. *Id.* at 393.

48. *Id.* at 386.

49. *Id.* at 394.

50. *Id.* at 395–96.

51. *Id.* at 395.

52. *Id.* at 394 ("[A] cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record.").

person would not be nearly as exhaustive.[53] Due to the unique nature of cell phones and digital data, the Supreme Court held that the incident to arrest exception to the Fourth Amendment does not apply to cell phones, and therefore a warrant is required.[54]

B. Carpenter v. United States

The Supreme Court did not end its discussion of digital data searches with *Riley*. In the 2018 case *Carpenter v. United States*,[55] the Court confronted whether the government could conduct a warrantless search of cell phone records to track an individual's movements.[56] The government accessed data showing the defendant's movements by searching his cell phone company's cell-site location information ("CSLI") records.[57]

The government argued that because the CSLI was collected by the cell phone company, the defendant did not have an expectation of privacy in that information and therefore a search of that information did not violate the defendant's Fourth Amendment rights.[58] The government based their argument on the third-party doctrine, which states that a person does not have a legitimate expectation of privacy in information knowingly shared or voluntarily conveyed with another, and therefore the individual cannot assert a Fourth Amendment violation against the government.[59]

The Court in *Carpenter* rejected the government's arguments,[60] holding that an individual maintains a legitimate expectation of privacy in the record of his physical movements, as captured through his cell phone and recorded by his cell phone company.[61] The Court in *Carpenter* grounded its analysis in whether an individual has a reasonable expectation of privacy in his phone.[62] The "reasonable expectation of privacy" test was first introduced in Justice Harlan's concurrence in *Katz v. United States*.[63] The majority in *Katz* established that the Fourth Amendment applies to "people, not places."[64] The test Justice Harlan proposed, which was later adopted by the Court,[65] is as follows: where an individual (i) holds a subjective expectation of privacy, and (ii) that expectation is objectively reasonable, the protections

53. *Id.* at 394–95.
54. *Id.* at 403.
55. 138 S. Ct. 2206 (2018).
56. *Id.* at 2211.
57. *Id.*
58. *Id.* at 2219.
59. *Id.*
60. *Id.*
61. *Id.* at 2219–20.
62. *Id.* at 2217–19.
63. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
64. *Id.* at 351 (majority opinion).
65. Smith v. Maryland, 442 U.S. 735, 740 (1979).

of the Fourth Amendment apply.[66] Put another way, where individuals and society expect privacy, searches within those spheres require a warrant.[67]

In *Carpenter*, the Court applied Justice Harlan's test to analyze how the Fourth Amendment should treat location data recorded by cell phones.[68] Though much cell phone data is shared with cell phone companies, which, according to the third-party doctrine, implies the information is not regarded as private,[69] the Court held that CSLI "is not truly 'shared' as one normally understands the term."[70] The Court explained that smart phones are pervasive and omnipresent[71] and that they carry *significantly* more information than traditional data composites like phone logs.[72] Additionally, the Court articulated that there is no practical way for the individual to prevent the collection of his location data by cell phone companies.[73]

The Court's pragmatic analysis in *Carpenter* indicates the Court's readiness to address the unique challenges electronic devices present to existing Fourth Amendment doctrine. Further demonstrating this point, the Court cited Justice Brandeis's "famous dissent" in *Olmstead v. United States*: "[T]he Court is obligated . . . to ensure that the 'progress of science' does not erode Fourth Amendment protections."[74] Together *Riley* and *Carpenter* set forth a strong defense for the protection of digital data from warrantless searches.[75] Given the Court's recognition of the privacy rights associated with electronic devices in *Riley* and *Carpenter*, and its consciousness of the implications technological advancements have to the preservation of Fourth Amendment protections in the digital age, important questions arise regarding how electronic devices ought to be treated at the border.

66. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
67. *See id.* at 360–61.
68. Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018).
69. *Id.*; *see supra* note 59 and accompanying text.
70. *Id.* at 2220.
71. *See id.* at 2218 ("While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales.").
72. *Id.* at 2219 ("There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today.").
73. *Id.* at 2220 ("Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data.").
74. *Id.* at 2223 (quoting *Olmstead v. United States*, 277 U.S. 438, 473–74 (1928) (Brandeis, J., dissenting)).
75. *Id.*

IV. SPLINTERING AMONG THE CIRCUITS

Reasonableness is at the core of how the border search exception should apply to electronic devices.[76] Recall that routine searches have been deemed reasonable per se because they occur at the border, whereas nonroutine searches must be justified by reasonable suspicion due to their high intrusiveness.[77] Electronic devices present challenges to privacy interests that traditional objects brought to the border do not, and so the question remains: Do forensic searches of electronic devices constitute nonroutine searches, and if so, what standard should border agents satisfy for a search of an electronic device to be considered reasonable?

The Ninth Circuit in *United States v. Cotterman*[78] and the Fourth Circuit in *United States v. Kolsuz*[79] held that forensic searches of electronic devices at the border are nonroutine searches and therefore require border agents to possess some level of suspicion before forensically searching electronic devices.[80] In contrast, the Eleventh Circuit in *United States v. Touset*[81] held that the border search exception applies normally to electronic devices and that no level of suspicion is required for forensic searches of electronic devices.[82] The analyses in *Touset*, *Kolsuz*, and *Cotterman* rest on three prominent factors: the intrusiveness of searching electronic devices, the ability of the traveler to mitigate the risk to his privacy interests, and how to balance the governmental interests at play.[83]

76. Riley v. California, 573 U.S. 373, 381–82 (2014) ("[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness.'") (quoting Brigham City v. Stuart, 547 U.S. 398, 403 (2006)).

77. Janes, *supra* note 27, at 76–77.

78. 709 F.3d 952 (9th Cir. 2013).

79. 890 F.3d 133 (4th Cir. 2018).

80. *See id.* at 144 (holding that a forensic border search of the defendant's phone required a showing of "individualized suspicion"); *see also Cotterman*, 709 F.3d at 968 (holding that a forensic border search examination of the defendant's computer required a showing of "reasonable suspicion"). Both the Fourth Circuit and the Ninth Circuit holdings only apply to forensic searches. Neither court extended their holding to manual, or cursory, searches. *Kolsuz*, 890 F.3d at 140 & n.2 (noting that the district court found a manual search to be a routine search, and therefore was reasonable per se, and that on appeal, Kolsuz expressly disclaimed any challenge to the manual search of his phone); *Cotterman*, 709 F.3d at 967 (stating that only a forensic search of an electronic device, not a manual review of its files, requires reasonable suslpicion).

81. 890 F.3d 1227 (11th Cir. 2018).

82. *Id.* at 1233 (holding that no suspicion is required for forensic searches of electronic devices at the border).

83. *See id.* at 1233–35; *Koluz*, 890 F.3d at 142–46; *Cotterman*, 709 F.3d at 962–67.

A. Intrusiveness of Searching Electronic Devices

i. Eleventh Circuit: Electronic Searches Are Not Intrusive Enough to Constitute a Nonroutine Search

Touset and Judge Smith's dissent in *Cotterman* held that the nature of the intrusiveness involved in searching electronic devices does not rise to the level of intrusiveness found in nonroutine searches.[84] *Touset* and Judge Smith distinguish searches of electronic devices from nonroutine searches by differentiating between searches of the person and searches of property.[85] Searches that have been considered nonroutine have concerned highly intrusive searches of the person, such as strip searches or x-ray examinations.[86] In contrast, various border search cases held reasonable suspicion was not required to search certain property, even when that property would ordinarily be considered private.[87] For example, *United States v. Alfaro-Moncada* held that a search of a crew member's living quarters on a cargo vessel at the border did not require reasonable suspicion,[88] and *United States v. Flores-Montano* held that border agents can remove and search a car's fuel tank without a requirement of reasonable suspicion.[89] The *Touset* court noted that these two cases involved property that would ordinarily be considered intrusive to search, and yet they did not meet the level of intrusiveness which requires individualized suspicion.[90] Consequently, the *Touset* court said that even though searches of electronic devices may be intrusive, because they are searches of property and not searches of the person, they do not rise to the level of nonroutine searches.[91]

Similarly, Judge Smith in his dissent in *Cotterman* likened searches of electronic devices to established routine searches at the border.[92] Judge Smith stated that reasonable suspicion is not required for border searches of papers, nor "their modern-day equivalent"—i.e. the files stored on electronic devices.[93] Like the court in *Touset*, Judge Smith concluded that

84. *Touset*, 890 F.3d at 1233; *Cotterman*, 709 F.3d at 982 (Smith, J., dissenting).
85. *Touset*, 890 F.3d at 1233–34; *Cotterman*, 709 F.3d at 982 (Smith, J., dissenting).
86. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985) (holding that reasonable suspicion was required for the prolonged detention of a person at the border suspected of smuggling contraband in her alimentary canal); *see also* United States v. Alfaro-Moncada, 607 F.3d 720, 729 (11th Cir. 2010) (noting that reasonable suspicion is required for highly intrusive searches of the person like a strip search or an x-ray examination at the border).
87. *Touset*, 890 F.3d at 1233.
88. 607 F.3d at 732.
89. 541 U.S. 149, 155 (2004).
90. *Touset*, 890 F.3d at 1233.
91. *Id.*
92. United States v. Cotterman, 709 F.3d 952, 982–83 (9th Cir. 2013) (Smith, J., dissenting).
93. *Id.* at 982.

reasonable suspicion is not required for border searches of property, including searches of electronic devices.[94]

ii. Fourth and Ninth Circuits: Electronic Searches Are So Intrusive as to Require Reasonable Suspicion

In contrast to *Touset*, the courts in *Cotterman* and *Kolsuz* did not restrict intrusive nonroutine searches solely to searches of the person.[95] Instead, the courts in *Cotterman* and *Kolsuz* based their holdings on the difference between electronic devices and traditional items found in luggage, holding that the private nature of the data stored on electronic devices makes forensically searching them so intrusive as to require reasonable suspicion.[96]

While *Cotterman* predated *Riley* and *Carpenter*, it cited similar concerns to those voiced in *Riley and Carpenter* about the comprehensive and sensitive nature of the information stored on electronic devices.[97] The court in *Cotterman* distinguished electronic devices from traditional luggage. Electronic devices contain "private and sensitive information"[98] that travelors do not intentionally pack.[99] In contrast, a travelor would need to make a conscious decision to pack more traditional objects, such as diaries or physical copies of bank statements, recognizing that the discrete sensitive information they contain would be accessible to border agents if carried to the border.[100]

Kolsuz, like *Cotterman*, held that searches of electronic devices at the border require reasonable suspicion.[101] Because *Kolsuz* followed *Riley*,[102] *Kolsuz* framed its analysis of border searches of electronic devices using *Riley*'s characterization of cell phones as quantitatively and qualitatively

94. *Id.* at 994.

95. *See* United States v. Kolsuz, 890 F.3d 133, 146 (4th Cir. 2018); *Cotterman*, 709 F.3d at 968.

96. *Kolsuz*, 890 F.3d at 146 (holding that a forensic border search of a phone is nonroutine, and requires individualized suspicion); *Cotterman*, 709 F.3d at 968 (holding that a forensic border search of a computer required a showing of reasonable suspicion).

97. *Cotterman*, 709 F.3d at 965.

98. *Id.* at 956.

99. *Id.* at 965 ("When carrying a laptop, tablet or other device . . . removing files unnecessary to an impending trip is an impractical solution given the volume and often intermingled nature of the files. It is also a time-consuming task that may not even effectively erase the files.").

100. *Id.* ("When packing traditional luggage, one is accustomed to deciding what papers to take and what to leave behind.").

101. *Kolsuz*, 890 F.3d at 146.

102. Note, *Kolsuz* did not follow *Carpenter—Kolsuz* (decided May 2018) was decided a month before *Carpenter* (decided June 2018).

unique.[103] *Kolsuz* found the degree of information stored on a cell phone[104] and the highly sensitive nature of some of that information[105] demonstrated that forensic searches of cell phones are intrusive in a way which searches of other traditional objects are not. Therefore, the intrusiveness of forensically searching electronic devices requires border agents to possess some level of suspicion before conducting such a search.[106]

iii. Intrusiveness Analysis Post-Carpenter

Recall that *Carpenter* found that an individual has a reasonable expectation of privacy in the record of his physical movements as captured through his cell phone.[107] The Court grounded its opinion in the constant usage of cell phones—which "faithfully follow[] [their] owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales"[108]—and the immense amount of information which cell phones store and collect, including "exhaustive chronicle[s] of location information."[109] *Carpenter*'s characterization of digital data[110] reasserts the Supreme Court's position from *Riley* that governmental access to vast amounts of an individual's digital data significantly threatens the privacy interests protected by the Fourth Amendment.

Riley and *Carpenter* unequivocally dispensed with the idea that electronic devices and digital data should be treated identically to other traditional objects in Fourth Amendment doctrine.[111] Both *Riley* and *Carpenter* declared that longstanding exceptions to the Fourth Amendment's warrant requirement do not apply squarely to searches involving digital data.[112] As such, *Touset*'s conclusory argument that electronic devices should receive the same treatment as other traditional objects at the border fails to adequately account for the Supreme Court's earlier holding in *Riley* that searches of digital data implicate different

103. *Kolsuz*, 890 F.3d at 144 ("[I]n light of the Supreme Court's decision in *Riley*, a forensic border search of a phone must be treated as nonroutine, permissible only on a showing of individualized suspicion.").

104. *Id.* at 145 ("The sheer quantity of data stored on smartphones and other digital devices dwarfs the amount of personal information that can be carried over a border . . . in luggage or a car.").

105. *Id.* (stating that smartphones and laptops contain highly personal and sensitive information including financial records, business records, medical records, and personal emails).

106. *Id.* at 146.

107. Carpenter v. United States, 138 S. Ct. 2206, 2217–18 (2018).

108. *Id.* at 2218.

109. *Id.* at 2219.

110. *Id.*

111. *See supra* Part II.

112. *Carpenter*, 138 S. Ct. at 2219–20 (third-party doctrine); Riley v. California, 573 U.S. 373, 386 (2014) (search incident to arrest).

privacy interests than searches of traditional objects.[113] *Kolsuz* and *Cotterman* anticipated *Carpenter*'s holding that individuals have significant privacy interests in their digital data.[114] The courts in *Kolsuz* and *Cotterman* thereby appropriately concluded that the forensic searches of electronic devices at the border are only reasonable if justified by reasonable suspicion.[115]

iv. Intrusiveness Analysis Empirically

The conclusion of *Kolsuz* and *Cotterman* is reinforced by empirical data which reveals the significant expectations of privacy people attribute to their electronic devices.[116] A study asked three hundred adults living in the United States to rate the intrusiveness of different types of searches that could occur at the border.[117] The results showed that more than 85 percent of participants expected content-related searches of their electronic devices to require at least reasonable suspicion.[118] For specifically *forensic* searches of electronic devices, a mere 8 percent of participants did not expect border agents to have to satisfy any standard before conducting the search.[119]

Furthermore, the study indicated that people held different expectations when it comes to searches of electronic devices as opposed to more traditional searches. For more traditional searches, such as conducting pat-downs, using drug-sniffing dogs, or opening luggage, the participants did not believe any level of suspicion was required.[120] However, the study found that the participants perceived searches of electronic devices to be among the most intrusive and the most revealing of sensitive information.[121] Therefore it follows that "[i]f body cavity and strip searches at the border

113. *See* United States v. Touset, 890 F.3d 1227, 1233 (11th Cir. 2018).

114. *Carpenter*, 138 S. Ct. at 2217.

115. *See* United States v. Kolsuz, 890 F.3d 133, 144 (4th Cir. 2018); United States v. Cotterman, 709 F.3d 952, 968 (9th Cir. 2013).

116. Matthew B. Kugler, *The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study*, 81 U. CHI. L. REV. 1165, 1166–67 (2014).

117. *Id.* at 1191.

118. The study measured a variety of content-related searches of electronic devices, such as searching a device's deleted files, e-mails, text messages, recent web searches, and recent calls. For all the types of content-related searches measured, more than 85 percent of participants expected border agents to be required to satisfy reasonable suspicion or obtain a warrant, before conducting the search. *Id.* at 1196–98. Regarding expectations about if a warrant is needed for searches, the study found only one content-related search where a majority of participants believed the search did not require a warrant from a judge. "For that single exception—a search of the recent call list—49.47 percent of participants still believed that a warrant was required." *Id.* at 1195–96.

119. Of the remaining 92 percent of participants, 78 percent expected that a warrant was required for forensic searches of electronic devices at the border. *Id.* at 1198.

120. *Id.* at 1196.

121. The most intrusive being strip searches and cavity searches. *Id.*

require reasonable suspicion because of the privacy and dignity concerns that they raise, so too should searches of electronic devices."[122]

While travelers' overall expectation of privacy over their belongings may be less at the border,[123] travelers nevertheless retain a strong expectation of privacy in their electronic devices at the border.[124] The study's empirical evidence, as well as the legal authority of the Supreme Court's opinions in *Carpenter* and *Riley*, bolster the conclusions of *Kolsuz* and *Cotterman* that searching electronic devices at the border should require at least a showing of reasonable suspicion.

B. Travelers' Ability to Mitigate the Intrusion

The second factor discussed by cases addressing border searches of electronic devices is the traveler's ability to mitigate the degree of intrusion into their privacy from their electronic devices.[125] Ultimately, while individuals can take precautions to protect their privacy, such as encrypting their files or traveling with a device other than their primary personal device, the only certain way to protect against forensic searches of electronic devices at the border is to leave their devices at home entirely—a solution which is impractical in the modern age.[126]

i. Just Leave It at Home

Touset stated that "the Fourth Amendment does not guarantee the right to travel without great inconvenience."[127] When traveling to the border, travelers are on notice that their belongings may be searched, "and they are free to leave any property they do not want searched . . . at home."[128] Because travelers have the option to travel without their electronic devices if they want to prevent the government from accessing their private data, they have the ability to mitigate the intrusion into their privacy.[129] If their electronic devices are simply not brought to the border, border agents cannot search them.

---

122. *Id.* at 1209.

123. United States v. Flores-Montano, 541 U.S. 149, 154 (2004) ("[O]n many occasions, we have noted that the expectation of privacy is less at the border than it is in the interior."). *But see* Riley v. California, 573 U.S. 373, 392 (2014) ("[D]iminished privacy interests do[] not mean that the Fourth Amendment falls out of the picture entirely.").

124. *See generally* Kugler, *supra* note 116 (discussing empirical data on travelers' expectations of privacy in their electronic devices at the border).

125. *See* United States v. Touset, 890 F.3d 1227, 1235 (11th Cir. 2018); United States v. Kolsuz, 890 F.3d 133, 145 (4th Cir. 2018); United States v. Cotterman, 709 F.3d 952, 956, 966 (9th Cir. 2013).

126. *See* discussion *infra* Parts III.B.ii, III.B.iii.

127. *Touset*, 890 F.3d at 1235.

128. *Id.*

129. *Id.*

ii. Leaving It at Home Is Impractial

The court's position in *Touset* is persuasive for traditional objects that travelers may decide to leave at home, such as diaries or bank statements, but the "just leave it at home" argument does not carry much weight with regard to electronic devices.[130] The court in *Kolsuz* held that, realistically speaking, it is unreasonable to expect travelers to travel without their electronic devices.[131] The beginning of the *Cotterman* opinion conveyed a similar sentiment, discussing the pervasiveness of electronic devices and the frequency with which they accompany travelers to the border, though it did not explicitly articulate the same analysis found in *Kolsuz*.[132]

The ubiquity of electronic devices discussed by *Cotterman* and *Kolsuz* echoes the language used by the Supreme Court in *Riley*[133] and *Carpenter*.[134] In those cases, the Court acknowledged that electronic devices like cell phones are not likely to be left behind.[135] As a Maryland district court described, mobile devices serve "as digital umbilical cords to what travelers leave behind at home or at work, indispensable travel accessories in their own right, and safety nets to protect against the risks of traveling abroad."[136] Consequently, it is unlikely that individuals possess any real choice to leave their electronic devices behind in order to mitigate the intrusion into their devices at the border.

The ubiquity and constancy of cell phones, and the impracticality of leaving them at home, is also supported by empirical data. Nearly every American adult owns a cell phone of some kind.[137] Eighty-one percent of Americans own a smartphone.[138] Fifty-two percent of Americans own a tablet computer.[139] A growing number of Americans use smartphones as

130. *Kolsuz*, 890 F.3d at 145.

131. *Id.* ("[W]hile an international traveler can mitigate the intrusion occasioned by a routine luggage search by leaving behind her diaries, photographs, and other especially personal effects, the same is not true, at least practically speaking, when it comes to smartphones and digital devices.").

132. The start of the *Cotterman* opinion reads: "Every day more than a million people cross American borders . . . . As denizens of a digital world, they carry with them laptop computers, iPhones, iPads, iPods, Kindles, Nooks, Surfaces, tablets, Blackberries, cell phones, digital cameras, and more." United States v. Cotterman, 709 F.3d 952, 956 (9th Cir. 2013).

133. Riley v. California, 573 U.S. 373, 395 (2014) ("Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception.").

134. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) ("While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales.").

135. *See Carpenter*, 138 S.Ct. at 2218; *Riley*, 573 U.S. at 395.

136. United States v. Saboonchi, 990 F. Supp. 2d 536, 557–58 (D. Md. 2014).

137. *Mobile Fact Sheet*, PEW RES. CTR. (June 12, 2019), http://www.pewinternet.org/fact-sheet/mobile [https://perma.cc/2MM2-6SP7] (noting 96 percent of Americans own a cell phone).

138. *Id.*

139. *Id.*

their primary means of online access at home and 17 percent of Americans use a smartphone as their only access to internet at home.[140] As a result, the "just leave it at home" argument is not a realistic solution to protecting travelers' privacy.

iii. Other Available Alternatives

Amidst the privacy debate on how electronic devices should be treated at the border, technology writers have discussed other methods that individuals can use to safeguard the data on the electronic devices at the border, aside from simply leaving their devices at home.[141] Such methods include traveling with a "travel device" (a device used only for traveling as opposed to a primary personal device),[142] backing up your data to the cloud and then erasing it from the local device,[143] logging out of apps,[144] not memorizing your passwords,[145] and protecting your data via encryption.[146] However, the effectiveness and practicality of these alternatives vary, and

140. *Id.*

141. *See* SOPHIA COPE ET AL., ELEC. FRONTIER FOUND., DIGITAL PRIVACY AT THE U.S. BORDER: PROTECTING THE DATA ON YOUR DEVICES *passim* (2017), https://www.eff.org/files/2018/01/11/digital-privacy-border-12-2017.pdf [https://perma.cc/M9JN-RY3X]; Christopher Elliott, *How Can You Protect Your Right to Digital Privacy at the Border?*, WASH. POST (June 8, 2017), https://www.washingtonpost.com/lifestyle/travel/how-can-you-protect-your-right-to-digital-privacy-at-the-border/2017/06/08/95c2cf3e-358f-11e7-b373-418f6849a004_story.html?noredirect=on&utm_term=.e70dbd98c637 [https://perma.cc/CN38-UBXF]; Brian X. Chen, *Crossing the Border? Here's How to Safeguard Your Data From Searches*, N.Y. TIMES (Mar. 21, 2017), https://www.nytimes.com/2017/03/21/technology/personaltech/crossing-the-border-heres-how-to-safeguard-your-data-from-searches.html [https://perma.cc/MM2F-9BV4].

142. Chen, *supra* note 141.

143. *Id.* This method mitigates risk to a traveler's privacy because it is CBP policy not to access data stored remotely on the cloud. *See* U.S. CUSTOMS & BORDER PROT., CBP DIRECTIVE NO. 3340-049A, BORDER SEARCH OF ELECTRONIC DEVICES 4 (2018) [herineafter CBP DIRECTIVE NO. 3340-049A] ("Officers may not intentionally use the device to access information that is solely stored remotely."); *see also* E.D. Cauchi, *Border Patrol Says It's Barred from Searching Cloud Data on Phones*, NBC NEWS (July 12, 2017, 9:53 PM), https://www.nbcnews.com/news/us-news/border-patrol-says-it-s-barred-searching-cloud-data-phones-n782416 [https://perma.cc/PD2J-TU9Z] ("U.S. border officers aren't allowed to look at any data stored only in the 'cloud'—including social media data—when they search U.S. travelers' phones, Customs and Border Protection acknowledged in a letter obtained Wednesday by NBC News.").

144. Chen, *supra* note 141.

145. For example, an individual could practice this method by allowing a friend to change the password to his device. The individual would recover the password for his device from his friend only after he has crossed the border. *Id.*

146. *Id.* "[E]ncryption is the method by which . . . data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key." Margaret Rouse et al., *Encryption*, SEARCHSECURITY (May 2019), https://searchsecurity.techtarget.com/definition/encryption [https://perma.cc/454Q-SD5A]. Programs, such as BitLocker, TrueCrypt, or Apple's Fivevault, allow individuals to encrypt data on their electronic devices. *See* Andy Greenberg, *A Guide to Getting Past Customs with Your Digital Privacy Intact*, WIRED (Feb. 12, 2017, 7:00 AM), https://www.wired.com/2017/02/guide-getting-past-customs-digital-privacy-intact/ [https://perma.cc/7TQX-VF7B].

the use of some of these alternatives may be ineffective in the context of forensic searches which have the ability, for example, to crack encryptions.[147] Ultimately, the only sure way to protect your data privacy, when the law does not afford protection, is to leave your devices at home[148]—which, as previously stated, is an unrealistic solution.[149]

C. Balancing Governmental Interests

The third major factor which the courts in *Touset*, *Kolsuz*, and *Cotterman* discuss is the weight that should be granted to the governmental interests at play at the border.[150] Exceptions to the Fourth Amendment's warrant requirement arise from instances where governmental interests outweigh individual privacy interests.[151] For the purposes of weighing privacy interests in electronic devices against governmental interests at the border, *Riley* and *Carpenter* provide guidance as to how strong the privacy interests are in electronic devices. In *Riley* the Court held that individuals' privacy interests in their cell phones outweighed the governmental interests in protecting officers' safety and in preventing the destruction of evidence.[152] In *Carpenter* the Court held that the privacy interests implicated in the "exhaustive chronicle" of location information amassed by cell phone companies outweighed the governmental interest in being able to obtain information without a warrant when an individual voluntarily shares that information with a third party and thus does not have a reasonable expectation of privacy over that information.[153] These cases demonstrate that the privacy interests in digital data are strong enough to outweigh governmental interests in other Fourth Amendment doctrine exceptions, and potentially strong enough to outweigh the significant governmental interests underlying the border search exception.

147. *See* NIJ FORENSIC EXAMINATION GUIDE, *supra* note 8, at 16.

148. Elliott, *supra* note 141.

149. *See* discussion *supra* Part III.B.ii.

150. *See* United States v. Touset, 890 F.3d 1227, 1235 (11th Cir. 2018); United States v. Kolsuz, 890 F.3d 133, 143 (4th Cir. 2018); United States v. Cotterman, 709 F.3d 952, 966 (9th Cir. 2013); *see also Kolsuz*, 890 F.3d at 152 (Wilkinson, J., concurring) (discussing the severity of the governmental interests at the border—"the point most freighted with security threats and the point at which a nation asserts and affirms its very right to nationhood").

151. *See* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) (discussing the third-party doctrine); Riley v. California, 573 U.S. 373, 385–93 (2014) (discussing the search incident to arrest exception); Wyoming v. Houghton, 526 U.S. 295, 299–307 (1999) (discussing the automobile exception and its application to containers found within the automobile); United States v. Montoya de Hernandez, 473 U.S. 531, 538–41 (1985) (discussing the border search exception).

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

153. *Carpenter*, 138 S. Ct. at 2219.

i. Governmental Interests at the Border

The origin of the border search exception was to allow the government to protect the country against "unwanted persons and effects,"[154] such as contraband, communicable disease, narcotics, explosives, and other threats to national security.[155] To justify applying the border search exception to forensic searches of electronic devices, the significant privacy interests implicated in suspicionless forensic searches must be outweighed by the governmental interests present at the border.

a. National Security Concerns Are Paramount

The governmental interests in searching electronic devices at the border involve national security interests, such as guarding against terrorism.[156] When balancing the interests of the government against the individual's right to privacy at the border, the balance is "struck much more favorably to the Government," due to the weighty interest the nation has in protecting itself from threats to its security.[157] Moreover, the CBP considers searches of electronic devices to be "essential to . . . detect evidence relating to terrorism and other national security matters."[158] Suspicionless forensic searches allow border agents broad discretion to act based on their professional experience without requiring them to delineate a justification for each search.[159] The broad discretion given to border agents to conduct suspicionless forensic searches creates a "powerful deterrent" for "technologically savvy terrorists and criminals."[160]

Touset held that the governmental interests present at the border outweighed the privacy interest travelers have in their electronic devices,[161]

154. United States v. Flores-Montano, 541 U.S. 149, 152 (2004) ("The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border.").

155. *Montoya de Hernandez*, 473 U.S. at 544.

156. CBP DIRECTIVE NO. 3340-049A, *supra* note 143, at 4. Governmental interests at the border include detecting and interdicting terrorists, drug smugglers, and human traffickers; preventing against the entry of dangerous goods, terrorist weapons, and contraband; and enforcing immigration laws. *Id.* (citing 6 U.S.C. § 211 (2012)); *see also* United States v. Cotterman, 709 F.3d 952, 985 (9th Cir. 2013) (Smith, J., dissenting) ("Terrorists rely on electronic storage devices, for example, to copy and alter passports and other travel documents.").

157. *Montoya de Hernandez*, 473 U.S. at 540. Also recall that the expectation of privacy is less at the border. *Flores-Montano*, 541 U.S. at 154. *But see Riley*, 573 U.S. at 392 ("[D]iminished privacy interests do[] not mean that the Fourth Amendment falls out of the picture entirely.").

158. CBP DIRECTIVE NO. 3340-049A, *supra* note 143, at 1.

159. *Cotterman*, 709 F.3d at 984 (Smith, J., dissenting).

160. *Id.* at 985.

161. The court stated, "We are . . . unpersuaded that a traveler's privacy interest should be given greater weight than the 'paramount interest [of the sovereign] in protecting . . . its territorial integrity.'" United States v. Touset, 890 F.3d 1227, 1235 (11th Cir. 2018) (alteration in original) (quoting *Flores-Montano*, 541 U.S. at 153).

stating that the government needs the ability to search electronic devices at the border to protect its border from the new threats to national security posed by technologically sophisticated criminals.[162] *Touset* reasoned that, in fact, the technological advancements in electronic devices and danger of technologically savvy criminals *necessitate* a lenient approach to searching electronic devices at the border.[163]

Additionally, Judge Smith's dissent in *Cotterman* weighed national security similarly to the *Touset* majority.[164] Judge Smith's dissent raised concerns about practical and administrative limits on the ability of border search agents to search electronic devices.[165] Judge Smith stated that it would be administratively impractical to expect border agents to determine what constitutes sufficient reasonable suspicion to forensically search an electronic device.[166] Judge Smith suspected that border agents, confused or uncertain about how to comply with a reasonable suspicion standard, would be reluctant to conduct a search out of fear of disciplinary hearings or a *Bivens* action,[167] thereby leaving the border vulnerable.[168]

b. Clarity of the Doctrine Is Valuable

Furthermore, Judge Smith identified that one advantage to squarely applying the border search exception to electronic devices is clarity and consistency of the law.[169] Departing from longstanding and well-defined areas of Fourth Amendment doctrine can cause confusion.[170] Applying the border search doctrine consistently to all searches of property at the border would give border agents surety that they are complying with the Fourth

162. *Id.* at 1235 ("If anything, the advent of sophisticated technological means for concealing contraband only heightens the need of the government to search property at the border unencumbered by judicial second-guessing.").

163. *Id.*

164. *Cotterman*, 709 F.3d at 981 (Smith, J., dissenting) ("I sincerely hope the Supreme Court will . . . reverse the holding in this case . . . for the sake of our national security, and the consistency of our national border search law.").

165. *Id.* at 984.

166. *Id.* at 982.

167. A *Bivens* action is a federal cause of action for an individual to recover damages from a federal officer who has violated his Fourth Amendment rights. *See* Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388, 397 (1971).

168. *Cotterman*, 709 F.3d at 986 (Smith, J., dissenting) ("The majority's reasonable suspicion requirement saddles border patrol agents with a 'Sophie's choice' between securing our nation, and protecting their own livelihoods. These misaligned incentives create unnecessary risk . . . .").

169. *Id.* at 984.

170. *See* Carpenter v. United States, 138 S. Ct. 2206, 2224 (2018) (Kennedy, J., dissenting) (stating that the majority's departure from the third-party doctrine with regard to cell-site records "unhinges Fourth Amendment doctrine," "draws an unprincipled and unworkable line" between types of records, and will "frustrate principled application of the Fourth Amendment").

Amendment, and lower courts clarity as to the contours of the legal doctrine.[171]

However, refusing to require reasonable suspicion to conduct a forensic search of an electronic device at the border solely for the sake of clarity and consistency of doctrine alone is not a persuasive argument. Clarity and consistency of doctrine come second to preserving individuals' constitutional rights under the Fourth Amendment.[172] Moreover, the border search exception already lacks consistency and clarity—border agents are already required to justify certain nonroutine border searches with reasonable suspicion.[173] Any disruption to the clarity of the border search exception doctrine has already been approved by the Supreme Court for searches classified as nonroutine. The present legal issue would merely require that same standard in another set of border searches: forensic searches of electronic devices.[174]

ii. Privacy Interests Outweigh the Governmental Interests

a. The Privacy Interests Implicated Are Serious

Unlike the court in *Touset*, the courts in *Cotterman* and *Kolsuz* held that the balance of the nation's governmental interests and travelers' privacy interests is best achieved by requiring reasonable suspicion to search electronic devices at the border.[175] As discussed previously, the privacy interests implicated in suspicionless forensic searches of electronic devices are significant.[176] Furthermore, while the sheer number of travelers affected by suspicionless forensic searches of their electronic devices may be small, as *Cotterman* stated, "It is the potential unfettered dragnet effect that is

171. *Cotterman*, 709 F.3d at 985 (Smith, J., dissenting).

172. *See Carpenter*, 138 S. Ct. at 2219 (refusing to mechanically apply the third-party doctrine to cell-site location information because of the immense privacy interests implicated in digital data); Riley v. California, 573 U.S. 373, 386 (2014) (declining to apply the incident to arrest warrant exception to searches of cell phones); *see also* Kyllo v. United States, 533 U.S. 27, 35 (2001) (rejecting a "mechanical interpretation" of the Fourth Amendment and holding that the government could not exploit technological advancements in thermal imaging to skirt Fourth Amendment protections); *Carpenter*, 138 S. Ct. at 2263–64 (Gorsuch, J., dissenting) ("[C]larity alone cannot justify the third party doctrine.").

173. *See* United States v. Flores-Montano, 541 U.S. 149, 155–56 (2004); United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985); *see also* Janes, *supra* note 27, at 77 (discussing how reasonable suspicion is required to conduct certain nonroutine border searches); Park, *supra* note 42, at 282 (discussing how highly intrusive searches at the border require a minimal showing of reasonable suspicion).

174. *See generally* United States v. Touset, 890 F.3d 1227 (11th Cir. 2018); United States v. Kolsuz, 890 F.3d 133 (4th Cir. 2018); *Cotterman*, 709 F.3d 952.

175. *Kolsuz*, 890 F.3d at 144; *Cotterman*, 709 F.3d at 968.

176. *See supra* notes 95–124 and accompanying text.

troublesome."[177] The mere lack of restrictions on the government to forensically search electronic devices at the border leaves travelers vulnerable to potential abuses of that power, which, in the context of electronic devices, implicate significant privacy interests.

b. The Reasonable Suspicion Requirement Is Not Overly Burdensome

Requiring border agents to satisfy reasonable suspicion before conducting a forensic search of an electronic device would not significantly impede the governmental interests underlying the border search exception because border agents have already been found to satisfy a reasonable suspicion requirement.[178] In *Cotterman*, during the initial security search of the defendant at the border, a Treasury Enforcement Communication System ("TECS") alert was triggered, indicating that the defendant had a prior conviction for child molestation, had traveled out of the country frequently, and was possibly involved in child sex tourism.[179] The alert was part of "Operation Angel Watch"—a program designed to investigate individuals suspected of carrying paraphernalia of child pornography.[180] The court in *Cotterman* held that the TECS alert for the defendant, the defendant's prior related conviction and frequent travels, the fact that the defendant was crossing from a country known for sex tourism, the presence of password-protected files on the defendant's computer, as well as the nature of the Operation Angel Watch program, taken together, constituted reasonable suspicion of criminal activity to support a forensic search on his electronic devices.[181]

In *Kolsuz*, the defendant was suspected of attempting to export firearm parts without a license.[182] After admitting he had firearm parts without a federal license, the defendant's smartphone was manually searched by border agents—a routine search that is per se reasonable—followed by a

177. *Cotterman*, 709 F.3d at 966. As it is, the number of searches of electronic devices at the border has increased significantly over just the past few years: in fiscal year 2015 about 8,500 electronic devices were searched; in fiscal year 2016, that number climbed to more than 19,000; in fiscal year 2017 there were over 30,200; and in fiscal year 2018 a total of 33,295 electronic devices were searched. Joint Statement of Stipulated Facts, Ex. 46 ¶ 13, Alasaad v. Nielsen, No. 17-cv-11730-DJC (D. Mass. Apr. 30, 2019).

178. *See infra* notes 185–190 and accompanying text.

179. *Cotterman*, 709 F.3d at 957. The Department of Homeland Security uses TECS to keep track of individuals crossing the border who are suspected of criminal activity. *Id.* at 957 n.3.

180. *Id.* at 958.

181. *Id.* at 969. The court made note that a discovery of password-protected files alone would not satisfy reasonable suspicion of criminal activity, but it could be considered together with other evidence of suspicious activity in the totality of circumstances. *Id.*

182. United States v. Kolsuz, 890 F.3d 133, 139 (4th Cir. 2018).

forensic search of the device.[183] The court held that the forensic search was supported by reasonable suspicion of criminal activity.[184]

As *Cotterman* and *Kolsuz* show, border agents have successfully satisfied the reasonable suspicion requirement without difficulty when conducting forensic searches of electronic devices.[185] Furthermore, various lower courts have also found reasonable suspicion was satisfied in border search cases, even if they did not hold that reasonable suspicion was necessary to conduct the search.[186] Since border agents have satisfied the reasonable suspicion standard in the past, without any guidance—from courts or otherwise—there is no reason to expect that border agents would not be able to continue to do so if this standard becomes mandatory.

Moreover it is unlikely that the standard of reasonable suspicion will impede border agents' ability to conduct searches.[187] Typically border agents only conduct forensic searches of electronic devices where reasonable suspicion is already present.[188] The plain reality of limited government resources forces border agents to be discerning when they decide to conduct a forensic search, meaning they likely would only expend the effort to conduct a forensic search of an electronic device when they already possess some suspicion.[189] The reasonable suspicion standard still leaves border agents with flexibility to employ common sense and rely on experience to conduct forensic searches where appropriate.[190]

183. *Id.*

184. *Id.*

185. *Id.*; *Cotterman*, 709 F.3d 952. Note that *Cotterman* and *Kolsuz* limit their holdings to just forensic searches of electronic devices. The courts do not extend the reasonable suspicion requirement to cursory or "manual" searches of electronic devices. *Kolsuz*, 890 F.3d at 141; *Cotterman*, 709 F.3d at 967.

186. Patrick E. Corbett, *The Future of the Fourth Amendment in a Digital Evidence Context: Where Would the Supreme Court Draw the Electronic Line at the International Border?*, 81 MISS. L.J. 1263, 1306–07 (2012); *see, e.g.*, United States v. Arvizu, 534 U.S. 266, 277 (2002) (finding reasonable suspicion present); United States v. Molina-Isidoro, 884 F.3d 287, 293 (5th Cir. 2018) (holding that if the border search was nonroutine and required reasonable suspicion, the border agents had requisite reasonable suspicion based on finding drugs in the defendant's luggage); United States v. Irving, 452 F.3d 110, 124 (2d Cir. 2006) (finding the search was supported by reasonable suspicion); United States v. Rogozin, No. 09-CR-379(S)(M), 2010 U.S. Dist. LEXIS 121162, at *8–9 (W.D.N.Y. Nov. 16, 2010) (finding the search satisfied reasonable suspicion, but not ruling on whether such a search required a reasonable suspicion standard); United States v. Verma, No. H-08-699-1, 2010 U.S. Dist. LEXIS 34559, at *12–13 (S.D. Tex. Apr. 8, 2010) (finding the evidence supported reasonable suspicion, even though no suspicion was required).

187. *Cotterman*, 709 F.3d at 967.

188. *Id.* at 967 n.14 ("As a practical matter, border agents are too busy to do extensive searches (removing gas tanks and door panels, boring holes in truck beds) unless they have suspicion." (quoting United States v. Chaudhry, 424 F.3d 1051, 1054 (9th Cir. 2005) (Fletcher, J., concurring))).

189. *Id.*

190. *Id.* at 967.

IV. RESOLVING THE CHAOS: REQUIRE REASONABLE SUSPICION – BETTER YET, GET A WARRANT

A. At a Minimum, Satisfy Reasonable Suspicion

Riley and *Carpenter* demonstrate the significant privacy interests implicated in searches of electronic devices.[191] In those cases, the Supreme Court has carved out privacy protections for digital data, in spite of applicable existing Fourth Amendment exceptions.[192] At the border, those same serious privacy interests are present when individuals travel with their electronic devices. The highly intrusive nature of forensically searching electronic devices demonstrates that forensic searches of electronic devices at the border constitute nonroutine searches, and thereby require a standard of reasonable suspicion.[193] Furthermore, because traveling without one's electronic devices is impractical, the individual has little ability to effectively mitigate the risk to their privacy at the border.[194] As such, it is imperative that the law creates additional safeguards within the border search exception for searches of electronic devices at the border. Requiring border agents to satisfy reasonable suspicion before conducting a forensic search of an electronic device would protect the serious privacy interests implicated in such searches while placing only a slight burden on the furtherance of the governmental interests present at the border.[195]

B. The Case in Favor of a Warrant

Even post-*Riley*, no case has held that more than reasonable suspicion is required to conduct a forensic search of an electronic device at the border,[196] and the Eleventh Circuit in *United States v. Vergara* expressly rejected a warrant requirement for forensic border searches of cell phones.[197] Nevertheless, privacy advocates like the Electronic Frontier Foundation

191. *See* discussion *supra* Part III.A.
192. *See* discussion *supra* Part II.
193. *See* discussion *supra* Part III.A.
194. *See* discussion *supra* Part III.B.ii.
195. *See* discussion *supra* Part III.C.ii.
196. United States v. Kolsuz, 890 F.3d 133, 147 (4th Cir. 2018) ("But there was no case suggesting that even more would be necessary—for a forensic search of a phone at the border or, indeed, for *any* border search, no matter how nonroutine or invasive. And that remains the case today: Even as *Riley* has become familiar law, there are no cases requiring more than reasonable suspicion for forensic cell phone searches at the border.").
197. United States v. Vergara, 884 F.3d 1309, 1312 (11th Cir. 2018). In *Vergara*, the defendant argued that evidence of child pornography obtained from a forensic search of his cell phone should be suppressed because the search was conducted without a warrant based on probable cause. The court held that forensic searches of cell phones at the border do not require a warrant or probable cause. *Id.* at 1312–13.

("EFF")[198] and the American Civil Liberties Union ("ACLU"),[199] as well as Judge Pryor's dissenting opinion in *Vergara*,[200] have argued in favor of requiring border agents to obtain a warrant based on probable cause in order to conduct a forensic search of an electronic device at the border.

Judge Pryor argued that the significant privacy interests implicated in electronic devices, balanced against the slight burden of getting a warrant, should require border agents to obtain a warrant before conducting a forensic search.[201] To support her stance, Judge Pryor cited the Supreme Court's characterization of cell phones in *Riley*, that cell phones are qualitatively and quantitatively different from traditional objects due to their immense storage capacity and the sensitive nature of the information stored on them.[202] Judge Pryor stated that "cell phones are fundamentally different from any object traditionally subject to government search at the border"[203] and that cell phones do not contain the physical contraband which border searches traditionally targeted.[204] In addition, Judge Pryor argued that the burden of obtaining a warrant is minimal.[205] Technological advancements have made the process of obtaining a warrant easier and faster.[206] Therefore, border agents should be required to obtain a warrant to conduct a forensic search of a cell phone.

Additionally, Fourth Amendment protections are not designed for ease of compliance or implementation.[207] Drawing from the Supreme Court's guidance in *Riley*,[208] weighing the highly intrusive nature of a forensic search of electronic devices against the slight burden of obtaining a warrant,

198. *See* Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Defendant-Appellant at 2, United States v. Molina-Isidoro, 884 F.3d 287 (5th Cir. 2018) (No. 17-50070) [hereinafter EFF Amicus Brief] ("[B]order agents should be required to obtain a probable cause warrant to search the data stored or accessible on a digital device.").

199. *See* Brief of Amici Curiae American Civil Liberties Union et al. in Support of Defendant-Appellant at 28, United States v. Kolsuz, 890 F.3d 133 (4th Cir. 2018) (No. 16-4687) [hereinafter ACLU Amicus Brief] ("This Court should hold that because searches of electronic devices seized at the border infringe deeply on privacy interests, such searches should only be permitted pursuant to a warrant or, at a minimum, probable cause.").

200. *Vergara*, 884 F.3d at 1313–19 (Pryor, J., dissenting) (holding that post-*Riley*, a forensic border search of a cell phone should require a warrant based on probable cause).

201. *Id.* at 1317.

202. *Id.* at 1318.

203. *Id.* at 1315.

204. *Id.* at 1317 (such as communicable diseases, narcotics, or explosives); *see also* EFF Amicus Brief, *supra* note 198, at 3 ("[S]earches of digital devices without a warrant and probable cause are not sufficiently 'tethered' to the narrow purposes justifying the border search exception: immigration and customs enforcement."). *But see* United States v. Touset, 890 F.3d 1227, 1233 (11th Cir. 2018) ("Border agents bear the same responsibility for preventing the importation of contraband in a traveler's possession regardless of advances in technology.").

205. *Vergara*, 884 F.3d at 1317 (Pryor, J., dissenting).

206. In some jurisdictions, warrant requests can be emailed to judges which can be signed and returned in less than fifteen minutes. *Id.* (citing Riley v. California, 573 U.S. 373, 401 (2014)).

207. *See supra* note 172 and accompanying text.

208. *Riley*, 573 U.S. at 385–92.

it is reasonable—and arguably preferable due to the severe implications to individuals' privacy—to require border agents to obtain a warrant before conducting a forensic search of an electronic device at the border. To borrow the Supreme Court's language in *Riley*, the solution is "accordingly simple—get a warrant."[209]

V. FURTHER CONSIDERATIONS

In addition to the topics addressed thus far in this Note, there are three additional considerations related to border searches of electronic devices which merit discussion. First, the cases at the center of this Note concern *forensic* searches of electronic devices, but should the reasonable suspicion standard also apply to manual searches? This question requires analysis of the difference between a forensic search and a manual search, and the privacy interests implicated in each.

Second, how do border agents treat travelers' password-protected devices at the border? Specifically, do travelers have to provide border agents with their cell phone or laptop passwords if asked, and what data can be accessed from password-protected devices if they refuse?

Third, what is the current status of this legal issue? A recent change to CBP policy may remove this legal issue from pressing legal debate, but even if the debate is removed from the courts, the pressing policy concerns between privacy and governmental interests at the border survive and the need to update Fourth Amendment doctrine in the wake of digital data remains imperative.

A. Manual Searches and Forensic Searches Compared

A forensic search uses forensic software to copy, analyze, and preserve data stored on a device.[210] This type of search gives the examiner access to all readable files, password-protected data, hidden or encrypted data, deleted files, metadata, and unallocated file space.[211] In contrast to a forensic search, a manual search of a cell phone, also referred to as a cursory search, accesses a device's contents "in the same way a typical user would."[212] None of the cases at the center of this Note held that manual searches are

209. *Id.* at 403.
210. United States v. Cotterman, 709 F.3d 952, 963 n.9 (9th Cir. 2013).
211. *See* NIJ FORENSIC EXAMINATION GUIDE, *supra* note 8, at 16.
212. United States v. Kolsuz, 890 F.3d 133, 140 (4th Cir. 2018) (quoting United States v. Kolsuz, 185 F. Supp. 3d 843, 853 (E.D. Va. 2016)).

nonroutine or that manual searches require reasonable suspicion at the border.[213]

The degree of information implicated in forensic searches, compared with information accessed by manual searches, may explain the courts' different treatment of the two types of searches. As *Cotterman* stated, "An exhaustive forensic search of a copied laptop hard drive intrudes upon privacy and dignity interests to a far greater degree than a cursory search at the border."[214]

But prominent privacy advocates have argued that manual searches, as well as forensic searches, should be treated as nonroutine searches because even manual searches grant the government access to large amounts of sensitive and private information.[215] Manual searches can be highly intrusive because they could reveal much of the same sensitive information as forensic searches—private messages, emails, call logs, apps, photographs, calendars, and more.[216] Because many of the privacy interests implicated during forensic searches are also present during manual searches, manual searches should also require some higher standard of reasonableness.[217]

---

213. United States v. Touset, 890 F.3d 1227, 1233 (11th Cir. 2018) (finding that a border search of personal property does not require suspicion, though the court did not directly address the issue of manual searches); *Cotterman*, 709 F.3d at 967 (stating that reasonable suspicion is only required for a forensic search and not a manual search); *Kolsuz*, 890 F.3d at 140 (noting that the district court acknowledged that the Fourth Circuit has treated a manual or cursory search of a computer at the border as routine, but because the defendant did not challenge the manual search evidence on appeal, the court did not consider the issue further); *see also* United States v. Vergara, 884 F.3d 1309, 1312 (11th Cir. 2018) (stating that because the evidence leading to the defendant's conviction only stemmed from the forensic search, the court did not consider the level of suspicion required to support the initial, manual search of the cell phones).

214. *Cotterman*, 709 F.3d at 966 (likening a forensic search to a "computer strip search"); *see also Vergara*, 884 F.3d at 1318 (Pryor, J., dissenting) ("[T]he extreme intrusion into privacy posed by a forensic cell phone search [is] well beyond the intrusion posed by a manual search . . . .").

215. *See* EFF Amicus Brief, *supra* note 198, at 19; ACLU Amicus Brief, *supra* note 199, at 13–14; *see also Cotterman*, 709 F.3d at 981 (Smith, J., dissenting) ("Why the use of computer software to analyze a hard drive triggers a reasonable suspicion requirement while a 'manual review' of the same hard drive requires no suspicion, is left unexplained.").

216. EFF Amicus Brief, *supra* note 198, at 16 ("'Manual' searches of digital data can access emails, voicemails, text messages, call logs, contact lists, photographs, videos, calendar entries, shopping lists, personal notes, and web browsing history, as well as cloud data via apps."); ACLU Amicus Brief, *supra* note 199, at 13 ("An agent may be able to click on an email application and read thousands of emails stored on remote servers, or do the same with a health application and see years' worth of data about heart rates, reproductive cycles, and more."); *see also* United States v. Saboonchi, 990 F. Supp. 2d 536, 547 (D. Md. 2014) (acknowledging that "a conventional computer search can be deeply probing and . . . has the potential to be invasive").

217. EFF Amicus Brief, *supra* note 198, at 19 ("[A]ll searches of digital data at the border are 'non-routine' and thus fall outside the border search exception because the government's conduct is the same: accessing to an unprecedented degree tremendous amounts of highly personal information."); ACLU Amicus Brief, *supra* note 199, at 13–14 ("[A]n officer without specialized training or equipment can conduct exhaustive keyword searches using the device's built-in search function, thereby achieving many of the goals of a forensic search with a fraction of the effort.").

B. The Effectiveness of Passwords

While a detailed discussion of whether border agents can force travelers to provide their passwords is beyond the scope of this Note, the effectiveness of passwords as privacy protection merits some discussion. The Fifth Amendment privilege protects individuals against self-incrimination even at the border.[218] Revealing a password is considered testimonial or communicative evidence which is protected by the Fifth Amendment.[219] Therefore, forcing the surrender of a password at the border could violate the Fifth Amendment.[220] However, despite the Fifth Amendment protection guaranteed to travelers, border agents possess legal ways of pressuring travelers to give up their passwords. Border agents can *in effect* coerce travelers to relinquish their passwords by detaining travelers[221] or confiscating their devices.[222]

The privacy implications of a traveler sharing his password with border agents vary depending on the type of search being conducted—forensic or manual—as well as the level of security afforded by a device's password protection. To conduct a manual search of a password-protected device—which the law currently considers a routine search[223]—border agents would need the device's password to access its contents.[224] If a traveler does not share his password (and the border agent is unable to guess it), the border agent would not be able to access the contents of the device via manual search, in which case a password would serve as an effective safeguard to

218. Schmerber v. California, 384 U.S. 757, 761 (1966).

219. *Id.*

220. That being said, in contrast to passwords, some electronic devices unlock via a fingerprint sensor, which may not be protected by the Fifth Amendment privilege. Law enforcement agents have been able to secure warrants to compel people to unlock their phones by fingerprint because, while a password is protected testimony under the Fifth Amendment, a fingerprint is not of a testimonial nature and may not receive Fifth Amendment protections. Yet, it is unclear how fingerprint sensors would be treated at the border. Due to the lack of clarity, technology writers advise travelers to fully power down electronic devices with fingerprint censors because the devices usually require a password or pin, not a fingerprint, when they power back up. *See* Chen, *supra* note 141.

221. *See* Kaveh Waddell, *A NASA Engineer Was Required to Unlock His Phone at the Border*, ATLANTIC (Feb. 13, 2017), https://www.theatlantic.com/technology/archive/2017/02/a-nasa-engineer-is-required-to-unlock-his-phone-at-the-border/516489/ [https://perma.cc/KW84-NPC2]; *see also* E.D. Cauchi, *What If U.S. Border Agents Ask for Your Cellphone?*, NBC NEWS (Apr. 4, 2017, 11:56 AM), https://www.nbcnews.com/news/us-news/what-if-u-s-border-agents-ask-your-cellphone-n742511 [https://perma.cc/TAV7-Z9VF] ("If you refuse a search, they can keep you at the border for hours . . . .").

222. CBP DIRECTIVE NO. 3340-049A, *supra* note 143, at 7 ("An Officer may detain electronic devices . . . for a brief, reasonable period of time . . . . Unless extenuating circumstances exist, the detention of devices ordinarily should not exceed five (5) days.").

223. *See supra* notes 212–214 and accompanying text.

224. Punam Singh Rogers & Emily Nash, *Border Searches of Your Electronic Devices—What Rights Do You Have?*, FOLEY HOAG LLP (Mar. 23, 2017), https://foleyhoag.com/publications/alerts-and-updates/2017/march/border-searches-of-your-electronic-devices [https://perma.cc/K5RL-ZB8W] ("[I]f you have a password and you do not provide that password to the agent conducting the search, the routine search may not be able to proceed any further.").

privacy interests despite the absence of a reasonable suspicion standard.[225] If, however, border agents can in essence compel travelers to reveal their passwords, any protection passwords offer against a manual search would be irrelevant and meaningless.[226]

In contrast to a manual search, a forensic search can bypass certain password protections and encryptions, thereby nullifying the protections passwords provide.[227] Depending on the sophistication of a device's encryption, it is conceivable that the encryption cannot be cracked by the government's forensic search.[228] However, technology writers caution that forensic searches of electronic devices by the government can successfully crack most encryptions.[229] The lack of protections provided by passwords and encryption during forensic searches of electronic devices makes a reasonable suspicion requirement all the more important to protect travelers' privacy interests.

C. Current Status of the Legal Issue

A recent change to CBP policy may remove this legal issue from pressing legal debate. The CBP amended its policy in 2018 to require border agents to have reasonable suspicion for an "advanced search"—a search where agents use devices or software to conduct a forensic search of a device.[230] This policy alteration may lessen the pressure on the Supreme Court to address the legal conflict by rendering the issue nonurgent.

---

225. *Id.*

226. *Id.*

227. *See* NIJ FORENSIC EXAMINATION GUIDE, *supra* note 8, at 16 (stating that the "logical extraction" stage may include extraction of password-protected, encrypted, and compressed data); *see also* Meg Graham, *Inside the Software Law Enforcement Uses to Get Into Your Phone*, CHI. TRIBUNE (Mar. 4, 2016, 5:30 AM), https://www.chicagotribune.com/bluesky/originals/ct-software-apple-iphone-nowsecure-susteen-bsi-20160304-story.html [https://perma.cc/GM4T-8XV5] ("When a phone is locked with a passcode, companies can run 'brute force' applications to open it."); Selena Larson, *How Cops Could Get Your Data Without Unlocking Your Phone*, CNN: BUS. (Nov. 10, 2017, 3:34 PM), https://money.cnn.com/2017/11/10/technology/apple-texas-shooting-iphone/index.html [https://perma.cc/S354-AQD2].

228. Dustin Volz, *FBI Chief Calls Unbreakable Encryption 'Urgent Public Safety Issue*,*'* REUTERS (Jan. 9, 2018, 9:13 AM), https://www.reuters.com/article/us-usa-cyber-fbi/fbi-chief-calls-unbreakable-encryption-urgent-public-safety-issue-idUSKBN1EY1S7 [https://perma.cc/2964-792P].

229. *See* Thomas Brewster, *The Feds Can Now (Probably) Unlock Every iPhone Model in Existence*, FORBES (Feb. 26, 2018, 10:20 AM), https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/1 [https://perma.cc/P3MD-SM6G] (discussing the vendor Cellebrite, which the U.S. government has used to unlock and extract data from mobile devices); *see also* Joseph Cox, *Cops Around the Country Can Now Unlock iPhones, Records Show*, VICE: MOTHERBOARD (Apr. 12, 2018, 4:52 PM), https://motherboard.vice.com/en_us/article/vbxxxd/unlock-iphone-ios11-graykey-grayshift-police [https://perma.cc/PS7N-3LCH] (discussing the tool GrayKey, which can be used to bypass encryption).

230. CBP DIRECTIVE NO. 3340-049A, *supra* note 143, at 5.

Yet, the new CBP policy has been criticized by privacy advocates for containing a large loophole for the reasonable suspicion requirement for advanced searches.[231] The policy states that border agents do not need reasonable suspicion for such a search when there is a "national security concern."[232] Privacy advocates worry that "national security concern" will be construed broadly, thereby nullifying any added protection the CBP had awarded to privacy interests.[233]

Nevertheless, the legal issue of how border searches of electronic devices should be treated continues to be grappled with by courts. Separate from the cases which constitute the circuit split discussed in this Note, the EFF and ACLU have a pending suit against the Department of Homeland Security on behalf of eleven travelers whose electronic devices were searched at the border without a warrant.[234] The case, *Alasaad v. Nielsen*, was filed in the District Court of Massachusetts and has the potential to be later appealed to the First Circuit Court of Appeals and beyond to the Supreme Court. The case will add a new dimension to the law of border searches of electronic devices, and if heard by the Supreme Court, could resolve the conflict in law.

CONCLUSION

The Supreme Court has already confronted the danger posed by the digital age to Fourth Amendment privacy protections in *Riley* and *Carpenter*. In those cases, the Supreme Court held that the significant privacy interests in digital data outweighed the governmental interests at

231. *See* Sophia Cope & Aaron Mackey, *New CBP Border Device Search Policy Still Permits Unconstitutional Searches*, ELEC. FRONTIER FOUND. (Jan. 8, 2018), https://www.eff.org/deeplinks/2018/01/new-cbp-border-device-search-policy-still-permits-unconstitutional-searches [https://perma.cc/YZ7Y-V9L4] ("U.S. Customs and Border Protection (CBP) issued a new policy on border searches of electronic devices that's full of loopholes and vague language and that continues to allow agents to violate travelers' constitutional rights."); *see also* Neema Singh Guliani, *Congress Can Stop Humiliating and Unconstitutional Device Searches at the Border*, ACLU (Jul. 13, 2018, 7:00 PM), https://www.aclu.org/blog/privacy-technology/privacy-borders-and-checkpoints/congress-can-stop-humiliating-and [https://perma.cc/VZL3-9FHV] ("CBP updated its guidance . . . but the new rules still have glaring loopholes and deficiencies.").

232. CBP DIRECTIVE NO. 3340-049A, *supra* note 143, at 5.

233. Cope & Mackey, *supra* note 231.

234. Complaint for Injunctive & Declaratory Relief, Alasaad v. Nielsen, No. 1:17-cv-11730-DJC, 2017 WL 4037436 (D. Mass. Sept. 13, 2017); *see also* Press Release, Elec. Frontier Found., EFF, ACLU Sue Over Warrantless Phone, Laptop Searches at U.S. Border (Sept. 12, 2017), https://www.eff.org/press/releases/eff-aclu-media-conference-call-today-announce-lawsuit-over-warrantless-phone-and [https://perma.cc/R9WA-UFN2]. At the time this Note was published, both parties had filed motions for summary judgment, but Judge Casper of the District Court of Massachusetts had not yet ruled on the pending motions.

play, and in so doing, the Supreme Court updated the Fourth Amendment doctrine to conform with the realities of the digital age.[235]

At the border, the Fourth and Ninth Circuits have taken their cue from *Riley* and held that border agents must have reasonable suspicion to forensically search electronic devices at the border.[236] However, the Eleventh Circuit upheld the traditional border search exception and held that suspicionless searches of electronic devices are per se reasonable by virtue of being at the border.[237]

Based on the Supreme Court's protective treatment of digital data in *Riley* and *Carpenter*, the high invasiveness of searching electronic devices, the traveler's inability to effectively mitigate the risk to their privacy, and the slight burden a reasonable suspicion standard places on governmental interests at the border, this Note proposes adopting, at a minimum, a reasonable suspicion standard for forensic searches of electronic devices at the border.

The law should go further to require a warrant based on probable cause to search electronic devices at the border because of extreme privacy interests implicated in searches of electronic devices.[238] Furthermore, the law should demand that the higher standard for searching electronic devices apply to manual and forensic searches alike because the information accessible during a manual search implicates many of the same privacy interests at issue in a forensic search.

Rebecca M. Rowland[*]

235. *See* Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018); Riley v. California, 573 U.S. 373, 386 (2014).

236. United States v. Kolsuz, 890 F.3d 133, 144 (4th Cir. 2018); United States v. Cotterman, 709 F.3d 952, 968 (9th Cir. 2013).

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

238. Though this view is not adopted by any court, a warrant requirement is advocated for by Judge Pryor in her dissent in *United States v. Vergara*, 884 F.3d 1309, 1317 (11th Cir. 2018) (Pryor, J., dissenting). Various pricavy advocates also believe a warrant should be required to forensically search electronic devices at the border. *See* EFF Amicus Brief, *supra* note 198, at 2; ACLU Amicus Brief, *supra* note 199, at 3.

* J.D. (2020), Washington University School of Law; B.A. (2016), Dartmouth College. Thank you to Professor Neil Richards for inspiring me to write on a topic in privacy law and for providing guidance throughout, and to everyone at the *Washington University Law Review* for their invaluable feedback during the publication process.