What Matters More: Preserving a Fundamental Right to Privacy or Tampering with Another's Dignity Through Searches Because of "Reasonable Suspicion"

Darianne De Leon
American University Washington College of Law
WHAT MATTERS MORE: PRESERVING A FUNDAMENTAL RIGHT TO PRIVACY OR TAMPERING WITH ANOTHER’S DIGNITY THROUGH SEARCHES BECAUSE OF “REASONABLE SUSPICION”

DARIANNE DE LEON*

Introduction ..................................................................................................................554
II. Background .............................................................................................................557
   A. The Fourth Amendment Right to Privacy and the Border Search Exception........557
   B. The Eleventh Circuit .........................................................................................560
   C. The Ninth Circuit ............................................................................................561
   D. The Fourth Circuit ..........................................................................................562
III. Analysis ................................................................................................................563
   A. The Eleventh Circuit Improperly Interpreted and Applied the Reasonable Suspicion Standard to Forensic Electronic Device Border Searches by Failing to Require Officers to Have Any Level of Suspicion to Perform These Searches, Which Violates an Individual’s Fundamental Privacy Rights. .........................................................563
      1. The Eleventh Circuit Disregarded its own Definition of “Intrusiveness” by Failing to Apply it to Electronic Device Border Searches and thus, Violated the Fourth Amendment.................................................................566
   B. The Ninth Circuit’s Interpretation and Application of the

* Darianne De Leon is a Juris Doctor candidate at American University Washington College of Law. She received her Bachelor of Arts degree in Political Science, Economics and Law from John Jay College of Criminal Law in 2015. She would like to thank her mother, Johann, for her continuous love and support throughout this process.
Reasonable Suspicion Standard Partially Aligns with the Fourth Amendment’s Protection of Privacy Rights, but should be Expanded to Include an Individualized Suspicion Standard for Electronic Border Searches.......571

C. The Fourth Circuit Properly Interpreted and Applied the Individualized Suspicion Standard Because Using that Standard Balances Both Government Interests and Individual Privacy Protection.................................575

IV. Policy Recommendations.................................................................581

Conclusion................................................................................................583

INTRODUCTION

The Fourth Amendment is included in the United States Bill of Rights to guarantee an individual’s right to privacy.1 Fourth Amendment protections consequently require law enforcement officers to secure a search warrant, justified by probable cause, to conduct lawful searches and seizures.2 However, there are several exceptions to the warrant requirement.3 The border search exception is one of these exceptions, permitting officers to lawfully screen individuals at an international border without probable cause or a warrant, so long as the search is reasonable.4

On August 25, 2009, the United States Department of Homeland Security (hereinafter “DHS”) issued a Privacy Impact Assessment (hereinafter “PIA”) mandating that travelers entering or exiting a United States border or its functional equivalent, such as an airport, would be subject to a search of their electronic devices by Customs Border Protection (hereinafter “CBP”) and Immigration and Customs Enforcement (hereinafter “ICE”) officers for

1. See generally Wayne R. LaFave, The Fourth Amendment: “Second to None in the Bill of Rights,” 30 ADVOCATE 5 1987) (reiterating the importance of the Fourth Amendment, explaining that the Amendment determines the kind of society in which we live, and is second to the Bill of Rights).

2. See U.S. CONST. amend. IV (stating, “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”).

3. See generally Jeanette Doran Brooks, Valid Searches and Seizures Without Warrants, INST. OF GOV’T (Nov. 2004) (explaining the different exceptions to the warrant rule such as: (1) Exigent circumstances; (2) Search incident to arrest; (3) Automobile searches; (4) Consent searches; (5) Border searches; (6) Open fields; (7) Plain view, and (8) Special needs).

the purpose of maintaining national security. Specifically, circuit courts are split as to whether reasonable or individualized suspicion is needed to lawfully conduct forensic electronic device searches at the border. Generally, officers conduct two types of searches at the border: routine or manual searches of electronic devices and forensic searches of electronic devices, commonly referred to as nonroutine searches. Manual searches of electronic devices at the border allow officers to unlock a traveler’s electronic device and scroll through their personal contact list, call log, messages, emails, and browsing history without requiring any level of suspicion as a prerequisite. Forensic searches of electronic devices are conducted away from the border and allow officers to connect a traveler’s electronic device to external equipment that extracts stored information from the device. The forensic search allows officers to

---


7. See United States v. Kolsuz, 890 F.3d 133, 133 (4th Cir. 2018) (referring to circuit cases that disagree on the legal standard of the border search exception).

8. See U.S. CUSTOMS AND BORDER PROTECTION: CBP DIRECTIVE NO. 3340-049A, BORDER SEARCH OF ELECTRONIC DEVICES (Jan. 4, 2018) (explaining the difference between a “basic” search and “advanced” search. Note, basic searches are also referred to as manual or routine search; an advance search is also referred to as forensic, extended or nonroutine searches).

9. See id. (stating that during a basic search, an officer may analyze information encountered at the border).

10. See id. (explaining that even if a forensic search is conducted away from the border, the search is still valid because most port-of-entries are not sourced with forensic
review, copy, and analyze contents of an electronic device without needing a warrant.11 While DHS maintains that a reasonable suspicion standard governs the forensic search, various circuit courts conclude differently when determining whether an individualized, reasonable, or no suspicion standard applies.12

This Comment argues that the Eleventh Circuit’s approach to analyzing forensic electronic device searches at the border is inconsistent with the Fourth Amendment’s protections against unreasonable searches because the court’s standard does not require any level of suspicion for electronic device searches and thus, denies privacy protections guaranteed to individuals.13 Part II examines the relationship between the government interest in promoting national security and an individual’s fundamental right to privacy during manual and forensic searches at the border.14 Part III argues that the Eleventh Circuit’s lack of any level of suspicion for forensic electronic device searches at the border violates the Fourth Amendment because electronic devices store an individual’s private and personal information, triggering fundamental privacy protections.15 Part IV recommends that circuit courts conform to a uniform, objective standard when conducting electronic device border searches by adopting the individualized suspicion standard used in United States v. Kolsuz.16 Part V concludes that the Eleventh Circuit’s approach in not requiring any level of suspicion to conduct electronic device border searches is unconstitutional and reiterates the need for circuit courts to uniformly apply an individualized suspicion

---

11. See id. (explaining that forensic searches are more advanced and are mandated to be performed in the presence of a supervisor).

12. See id. (explaining that officers are allowed to perform an advanced search where there is reasonable suspicion such that there is a threat to national security).


14. See U.S. CONST. amend. IV (emphasizing the fundamental right to protect one’s self); see generally United States v. Ortiz, 422 U.S. 891, 891 (1975) (emphasizing that the purpose of the Fourth Amendment “is to protect liberty and privacy from arbitrary and oppressive interference by government officials”); Katz v. United States, 389 U.S. 347, 350 (1967) (reiterating the constitutional basis of the Fourth Amendment “person’s general right to privacy . . . to be let alone”).

15. See infra Part III (demonstrating the courts should develop a stream-lined procedure and process for border searches that are not subjective based on CBP officers).

16. See infra Part IV (explaining that the Supreme Court has the power to overturn the Eleventh Circuit’s application of the Fourth Amendment along the border while conducting electronic device searches).
standard when conducting these types of searches.17

II. BACKGROUND

A. The Fourth Amendment Right to Privacy and the Border Search Exception

The Fourth Amendment prohibits unreasonable searches and seizures against one’s person, property, and effects.18 A court needs to analyze the reasons for initiating the search and the scope of the search to determine reasonableness.19 Evolving caselaw has determined that border officials may lawfully conduct searches without a warrant so long as the search is reasonable.20 Reasonable suspicion requires border officials to have reason or cause to suspect that contraband exists in the particular place being searched.21 On the other hand, individualized suspicion is centralized on law enforcement officers making judgments based on a person’s unique actions, character, and situation.22 Individualized suspicion is designed to eliminate assumptions based on stereotypes, race, religion, and socio-economic background.23

The increase in technology has led to controversy in the legality of border searches involving electronic devices under the Fourth Amendment.24 Under

17. See infra Part IV (concluding that the Supreme Court should review and extend their Riley decision to searches of electronic devices at the border).

18. See U.S. CONST. amend. IV (stating, “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”).

19. See Katz, 389 U.S. at 357 (stating that searches conducted without a warrant are unlawful).

20. See United States v. Touset, 890 F.3d 1227, 1229 (11th Cir. 2018) (concluding with precedent that border searches are part of the warrantless exception rule and do not require anything else but reasonable suspicion to conduct a search of an electronic device at the border).

21. See United States v. Vega-Bravo, 729 F.2d 1341, 1351-52 (11th Cir. 1984) (Hatchett, J., dissenting) (explaining that the reasonable suspicion standard is usually used when a subject behaves in a suspicious manner).


23. See id. (reiterating that individualized suspicion requires examining both reasonable suspicion and probable cause).

24. See Riley v. California, 537 U.S. 373, 403 (2014) (holding that a warrantless digital search of a person’s cell phone is unconstitutional and violates the Fourth Amendment); see also Arizona v. Gant, 556 U.S. 332, 332 (2009) (holding that the search
the border search exception, CBP officers are allowed to conduct warrantless searches of travelers and their belongings to protect national security.25

The border search exception to the Fourth Amendment first emerged in United States v. Ramsey.26 In Ramsey, the defendant transported drugs into the United States via mail.27 The Supreme Court concluded that mail entering the United States is subject to the border search exception.28 The Court reasoned that the sole purpose of the border search exception is to protect the sovereign and thus, the mode of transportation does not matter.29 Merely crossing the border is sufficient for an officer to conduct a lawful search without needing probable cause or a warrant.30

In United States v. Kolsuz, the Fourth Circuit concluded that individualized suspicion is necessary when conducting a forensic search of electronic devices at the border because these searches are highly intrusive.31 In Kolsuz, border patrol detained the defendant at Washington Dulles Airport of a defendant’s vehicle while handcuffed in a patrol car was unreasonable; even though the facts of this case are different from the typical electronic device search cases, it is still applicable because most travelers who are stopped at the border feel as though they cannot “freely” remove themselves from a CBP officer; United States v. Kolsuz, 890 F.3d 133, 133 (4th Cir. 2018) (explaining that a forensic search of a traveler’s electronic device at the border is only permissible if the officer has reasonable suspicion).


26. See United States v. Ramsey, 431 U.S. 606, 606-07 (1977) (holding that customs inspector had reasonable cause to suspect that there was merchandise or contraband in the envelopes).

27. See id. at 609 (describing the transcontinental transportation of drugs into the United States by the defendant. Noting that the envelopes were heavier and fatter than regular mail).

28. See id. at 607 (stating that when mail crosses the border, probable cause is not needed to search the contents of the mail).

29. See id. at 606-07 (explaining that the border search exception is grounded in the recognized duty to protect the sovereign; moreover, the border exception is not an extension of the exigency doctrine).

30. See id at 618. (emphasizing that entering [and exiting] the country makes a resulting search “reasonable”).

while attempting to board an international flight to Turkey in 2016.\(^\text{32}\) Before the border officers searched the defendant’s electronic devices, the officers searched his luggage, revealing restricted firearm parts.\(^\text{33}\) After the border patrol searched the defendant’s luggage, he admitted that he was transporting firearm parts without a license and the officers arrested him.\(^\text{34}\) The court noted that the arrest did not preclude the border search exception because the defendant was at the functional equivalent to a border, the airport.\(^\text{35}\) Prior to his arrest, Kolsuz was well-known to government authorities; in 2012 and 2013 agents found illegal firearm parts in his luggage while traveling between Miami and Turkey.\(^\text{36}\) On both occasions, agents explained to him that he needed to comply with the licensing requirements to transport such equipment.\(^\text{37}\) In 2016, CBP agents used Kolsuz’s history and his third attempt to cross the border with illegal contraband as sufficient evidence to forensically search his electronic devices.\(^\text{38}\) The court concluded that CBP’s forensic search was based on individualized suspicion because they had “good” reason to support their notion that Kolsuz was attempting to export illegal contraband, the paramount basis for the border search exception.\(^\text{39}\) Alternatively, the Ninth Circuit concluded that border patrol needs reasonable suspicion, rather than individualized suspicion to conduct a forensic search.\(^\text{40}\) Furthermore, the Ninth Circuit reasoned that individualized suspicion is not required for border searches involving

\begin{itemize}
  \item \textit{See Kolsuz, 890 F.3d at 139} (explaining that the defendant had been warned twice before his arrest of the mandatory requirements for transporting firearms).
  \item \textit{See id.} at 139 (explaining that because of the defendant’s prior history, an email was sent to airport agents alerting them to be aware that the same illegal transportation of goods could occur).
  \item \textit{See id.} (noting that Agent Cogan and Budd found 18 handguns barrels, calibers, and a conversion kit).
  \item \textit{See id.} at 143 (stating that regardless of Kolsuz’s arrest, the border search exception still applies because he was exiting the functional equivalent of a border).
  \item \textit{See id.} at 140 (providing the history of Kolsuz to help show that he was pre-warned of the required license twice before his actual arrest).
  \item \textit{See id.} at 140-41 (showing that regardless of the warnings, Kolsuz had the intent to continue transporting illegal goods at the border).
  \item \textit{See id.} at 140-41 (explaining that the forensic search revealed a 900-page report of Kolsuz’s electronic device history).
  \item \textit{See id.} at 143 (stating that Kolsuz’s history shows that he intended to violate the protection of the United States therefore, he posed a national security risk).
  \item \textit{See United States v. Cotterman, 637 F.3d 1068, 1074 (9th Cir. 2011), aff’d on reh’g, 709 F.3d 952, 957 (9th Cir. 2013) (en banc)} (stating that the CBP officers relied on ICE’s confirmation that electronic media can be searched without individualized suspicion).
\end{itemize}
electronic devices because ICE published an official memorandum reaffirming that officers may seize electronic media at the border without having individualized suspicion.\textsuperscript{41} In sharp contrast to both the Fourth and Ninth Circuits, the Eleventh Circuit emphasized that CBP officers do not need to justify any form of electronic device search at the border, and thus, no reasonable or individualized suspicion is required.\textsuperscript{42}

B. The Eleventh Circuit

Traditionally, law permitted warrantless border searches simply because they occurred at the border.\textsuperscript{43} However, technology advances have changed this rhetoric.\textsuperscript{44} In United States v. Touset, the defendant made several money transfers from a Western Union account to a Philippines-based phone number to further sex tourism and child pornography in the country.\textsuperscript{45} Law enforcement became aware of the defendant’s illegal engagements via private investigations.\textsuperscript{46} While at the border, the CBP officers manually inspected the defendant’s electronic devices, but no child pornography was found.\textsuperscript{47} The officers seized and searched the defendant’s two laptops and external hard drives.\textsuperscript{48} The defendant argued that forensic searches of

\textsuperscript{41} See id. (stating customs officers acted presumptively without considering the level of suspicion because they relied on ICE’s manual for reaffirmation that individualized suspicion was not needed).

\textsuperscript{42} See United States v. Touset, 890 F.3d 1227, 1229 (11th Cir. 2018) (arguing that the courts’ precedent on border searches makes clear that no suspicion is necessary to search electronic devices at the border).

\textsuperscript{43} See United States v. Ramsey, 431 U.S. 606, 611 (1977) (reiterating the standard of protecting government interests and preventing national security risks at the border).

\textsuperscript{44} See U.S. Customs and Border Protection: CBP Directive No. 3340-049A, supra note 8 (explaining that as the use of technology increases, so does the strictness of our border laws).

\textsuperscript{45} See Touset, 890 F.3d at 1230 (providing additional detail about the investigations conducted against Touset: Touset made frequent low money transfers and created an “iloveyousomuch0820@yahoo.com” email account to document his transfers to clients in child pornography).

\textsuperscript{46} See id. at 1230 (stating that several private organizations and government agencies investigated Touset’s whereabouts and suggested that he had been involved with the transportation of child pornography. These organizations included “Xoom” and Cyber Center investigation team).

\textsuperscript{47} See id. (asserting that even though through a manual search no contraband was found, the agents still conducted a forensic search without having reasonable suspicion).

\textsuperscript{48} See id. (noting that CBP Officer Escobar did not find traces of child pornography when he performed a manual inspection of Touset’s two iPhones, a camera, and two tablets. Escobar returned the items to Touset and sent the additional electronic devices to a different agency to perform a forensic search).
electronic devices required reasonable suspicion. The Eleventh Circuit rejected the defendant’s argument, and ruled that no form of suspicion is required to search electronic devices at the border. The court followed the reasoning in Ramsey by concluding that searches at the border are reasonable when CBP agents have knowledge of illegal goods crossing a United States border or its functional equivalent. For example, both Ramsey and Touset involved defendants having a history with a country that was known to traffic either illegal narcotics (Ramsey) or child pornography (Touset). Moreover, the Ramsey Court concluded that by now, it is not necessary to require any additional explanation for suspicionless border searches because it only matters that they occur at the border.

In Touset, the court created a three-part test to determine whether a search was intrusive. To find that a search is intrusive, there must be: 1) physical contact between the searcher and person; 2) exposure of intimate body parts; and 3) use of force.

C. The Ninth Circuit

In 2013, the Ninth Circuit reheard United States v. Cotterman, a case in which the government had a lookout alert on the defendant for child pornography and molestation. CBP agents conducted two searches at the border. The first search included a vehicle search, during which the agents

49. See id. (stating that Touset relied on the Supreme Court’s holding in their Riley v. California decision).
50. See id. at 1229 (relying on the border exception to the Fourth Amendment).
51. See id. (explaining that the sole purpose of the border exception is to protect against national security risks).
52. See id. at 1232 (reiterating that border searches are different; officers are required to prevent contraband from entering the border).
53. See United States v. Ramsey, 431 U.S. 606, 616 (1977) (explaining that the suspicionless border searches have been a long-standing right of the sovereign; therefore, no further explanation is needed).
54. See Touset, 890 F.3d at 1234 (listing the elements that are most prevalent to identify whether a person’s dignity was violated).
55. See id. (emphasizing that these elements help to identify whether a forensic search was intrusive).
56. See United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013) (noting that Howard Cotterman was a registered sex offender in the state of California, and was convicted for two counts of sexual misconduct against a minor).
57. See id. at 957-58 (stating that the first search fell within the Fourth Amendment border exception, and therefore the second search was just an extension of the first search even though it was performed away from the border).
discovered two laptop computers and three digital cameras. The second search involved manual inspection of the defendant’s electronic devices. The search did not reveal any child pornography on the devices, mainly because the electronic devices were password protected. At this time, the CBP agent seized the defendant’s laptop for a forensic search, which was conducted 170 miles away from the original border search. The defendant offered to help the CBP Agent unlock the computer by providing the password, but the Agent refused because she feared that the defendant would tamper with the evidence. The Ninth Circuit concluded that CBP agents must have reasonable suspicion before administering a forensic search of an electronic device at the border. The court reasoned that while the border search exception’s purpose is to protect government interests, reasonable suspicion is needed so that the government cannot seize property on a “whim” for an indefinite period of time.

D. The Fourth Circuit

Given the extensiveness of a forensic electronic device search, the Fourth Circuit takes the Ninth Circuit’s holding one step further by concluding that officers must have individualized suspicion before conducting device searches of forensic electronics at the border. In Kolsuz, CBP officers

58. See id. at 957; see also 19 U.S.C. § 1433(b) (2010) (noting that vehicles entering the United States are subject to an inspection and detention if necessary).

59. See id. (explaining that the agent used Cotterman’s history of transporting child pornography to justify the manual search of his electronic device).

60. See CBP DIRECTIVE No. 3340-049, at 5.3.2.2 Technical Assistance – With or Without Reasonable Suspicion, (Aug. 25, 2009) (acknowledging that during an electronic device search, officers may encounter technical issues such as password protection that require them to transmit copies of information for further federal agency assistance).

61. See Cotterman, 709 F.3d at 956 (noting that the original search at the border did not uncover any incriminating material).

62. See id. at 958 (finding that Agent Riley had three concerns: (1) Cotterman could delete the files, without her knowledge; (2) laptops might be “booby trapped”; and (3) she would be unable to access files).

63. See id. at 968 (finding that the intrusive nature of forensic searches created a reasonable suspicion requirement; United States v. Alfonso, 759 F.2d 728, 734 (9th Cir. 1985) (holding that the “extended border searches must be justified by ‘reasonable suspicion’”).

64. See Cotterman, 709 F.3d at 957 (showing the court’s reluctance to equate the border exception as an “anything goes” policy).

65. See United States v. Kolsuz, 890 F.3d 133, 144 (4th Cir. 2018) (stating that individualized suspicion is a higher requirement to meet and focuses on how intrusive the search was).
detained a Turkish national when they found firearm parts in his luggage as he attempted to cross the border.\footnote{See \textit{id.} at 139 (explaining that defendant tried to smuggle firearms out of the country without a license).} Upon the defendant’s arrest, the agents seized the defendant’s smartphone and performed a month-long forensic search.\footnote{See \textit{id.} at 141 (noting that the defendant was in custody for the duration of the forensic search).} The Government asserted that the thirty-day forensic search was lawful because it had reasonable suspicion that a crime had already occurred or was about to occur.\footnote{See \textit{id.} at 143 (noting that the district court emphasized that a “nonroutine” search of electronic devices at the border is justified by reasonable suspicion).} The defendant argued that the forensic search was unconstitutional because the government performed the search without a warrant.\footnote{See \textit{id.} at 142 (explaining that if the border search exception did not apply to this search, standard Fourth Amendment rules would apply).} The defendant further argued that because the government conducted the forensic search away from the border, the law should exclude it from the exception.\footnote{See \textit{id.} (noting the courts’ holding that regardless of distance and proximity to the border, the border search exception still applies).} The Fourth Circuit held that CBP agents are permitted to conduct electronic device searches at the border—conditioned upon the agents having individualized suspicion; and, in \textit{Cotterman}, the agents’ reliance on the firearm parts provided sufficient evidence of potential criminal activity based on individualized suspicion.\footnote{See \textit{id.} at 143-44 (asserting that forensic border search of cell phones must be treated as a nonroutine border search which is permissible only upon showing of individualized suspicion).}

Furthermore, the court agreed with \textit{Cotterman}’s reasoning that a search’s proximity to the border is irrelevant and does not bar the search.\footnote{See \textit{Kolsuz}, 890 F.3d at 142 (stating that a forensic border search can be conducted days after a manual search and miles away from the border).}

III. ANALYSIS

\textbf{A. The Eleventh Circuit Improperly Interpreted and Applied the Reasonable Suspicion Standard to Forensic Electronic Device Border Searches by Failing to Require Officers to Have Any Level of Suspicion to Perform These Searches, Which Violates an Individual’s Fundamental Privacy Rights.}

Under the border exception to the Fourth Amendment, an officer may lawfully conduct a search at the border so long as the search is reasonable.\footnote{See CBP \textsc{DIRECTIVE} NO. 3340-049A, \textit{supra} note 8 (explaining the expectation}
In *Touset*, the Eleventh Circuit held that officers can perform forensic electronic device searches at the border without any level of suspicion.\(^{74}\) While the Eleventh Circuit does not address manual electronic device searches, it unconstitutionally determined that officers conducting forensic searches of electronic devices at the border never require reasonable or individualized suspicion.\(^{75}\) Applying the new standard, in *United States v. Vergara*, the Eleventh Circuit concluded that officers conducting forensic searches of electronic devices at the border do not require probable cause or a warrant.\(^{76}\) The Eleventh Circuit’s reasoning relies on its precedent and the First Congress’s intended purpose of the Fourth Amendment.\(^{77}\) According to the Eleventh Circuit, the First Congress empowered customs officials to conduct warrantless stops and searches of any vessel or cargo suspected of transporting illegal goods at the border or its functional equivalent.\(^{78}\)

The Eleventh Circuit fails to consider the significance and connection between modern electronic devices and a traveler’s right to privacy at the border.\(^{79}\) The Eleventh Circuit’s legal standard is inconsistent with the Fourth Amendment because it fails to recognize that cell phones, computers, and other electronic devices require the same Fourth Amendment protections as a home.\(^{80}\) Presently, most people store all of their personal and

---

74. See *United States v. Touset*, 890 F.3d 1227, 1233 (11th Cir. 2018) (stating that the Fourth Amendment does not require any suspicion for forensic searches of electronic devices at the border), see also *United States v. Vergara*, 884 F.3d 1309, 1310 (11th Cir. 2018) (asserting that the border search exception allows for a lower standard of reasonable suspicion).

75. See *Touset*, 890 F.3d at 1234 (citing *United States v. Ramsey*, 431 U.S. 606, 616 (1977)) (distinguishing searches of property from searches of one’s person).

76. See *Vergara*, 884 F.3d at 1312 (stating that the Court’s rhetoric has existed long before the Fourth Amendment and only searches that are “highly intrusive” to the body require a reasonable suspicion requisite).

77. See *Touset*, 890 F.3d at 1236 (explaining that the Eleventh Circuit relies on precedent to conclude that warrantless forensic searches of electronic devices are permissible at the border because they are not highly intrusive nor bodily).

78. See id. (stating that the Eleventh Circuit relies heavily on the historical importance of Congress’s intention to create a border search exception, even when electronic devices were not popularly used or even invented).

79. See id. at 1233 (stating that a traveler’s right to be left alone does not prevent the search of traveler’s luggage and materials).

80. Compare id. (reiterating that the Eleventh Circuit does not distinguish between border searches of different kinds of property) with *United States v. Kolsuz*, 890 F.3d 133, 145 (4th Cir. 2018) (explaining that electronic devices that contain highly personal information are ubiquitous and require Fourth Amendment protection).
professional information on a portable electronic device and thus, courts should consider it as an “effects” under the Fourth Amendment’s privacy protections.\(^\text{81}\)

Moreover, the Eleventh Circuit incorrectly concludes that a forensic search of an electronic device at the border is not intrusive.\(^\text{82}\) The court reasons that because a forensic electronic device search does not involve an agent touching or exposing the suspect’s body parts, the search is not intrusive.\(^\text{83}\) The Eleventh Circuit’s application of the legal standard violates the Fourth Amendment because it allows officers to subjectively determine when to conduct a forensic search without ever having reasonable suspicion.\(^\text{84}\) Instead, the court relies solely on the notion that the border search exception emerged to protect government interests only.\(^\text{85}\) The court’s reasoning disregards an individual’s privacy rights under the Fourth Amendment.\(^\text{86}\)

Furthermore, the Eleventh Circuit’s suspicionless border search standard is not inclusive nor practical to apply.\(^\text{87}\) The court fails to realize the intimate relationship between a traveler and his electronic device.\(^\text{88}\) Electronic

81. See Kolsuz, 890 F.3d at 145-46 (citing Riley v. California, 573 U.S. 373, 400 (2014)) (highlighting the differences between cell phones and other kinds of property); see also U.S. CONST. amend. IV (stating, “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”).

82. See Touset, 890 F.3d at 1233-34 (using the court’s precedent to conclude that a search of a person’s body is the only kind of search that requires individual suspicion).

83. See id. at 1234; Riley v. California, 573 U.S. 373, 393 (2014) (explaining that under the search incident-to-arrest doctrine, an additional search of one’s pocket bears no additional privacy intrusion but searching one’s digital devices has a substantially greater privacy interest and thus a higher level of intrusion).

84. See Touset, 890 F.3d at 1237 (noting that while reasonable suspicion is based on an objective inquiry, reasonable suspicion is not required for searches of electronics at the border).

85. See id. at 1235 (stating that the court is unpersuaded that an individual’s right to privacy is not given more weight than the paramount interest of the sovereign).

86. See id. at 1233 (re-asserting that not even the Supreme Court has required reasonable suspicion to search a traveler’s property at the border). But cf. Riley, 573 U.S. at 396-97, 2491 (noting that searches of cell phones implicate different privacy concerns than searches of property like luggage because electronic devices may contain more information than would even be found in a typical search of a home).

87. See Touset, 890 F.3d at 1228 (reasoning that although many people own electronic devices, forensic searches of devices are not intrusive because the device is property, not a traveler’s person or body).

88. See id. at 1233 (comparing the information contained on cell phones to that contained in “a tractor-trailer loaded with boxes of documents”).
devices store vast amounts of information and a cell phone search exposes the government to far more information than the most intrusive search of a house. 89 The attachment between a traveler and his electronic device is significant for Fourth Amendment purposes because the traveler may store information that could potentially expose his family and profession. 90 A suspicionless forensic search of this information can result in harmful consequences. 91 For example, Justice Sotomayor emphasized in her Riley concurrence that cell phones store large amount of applications, that when forensically searched, can reveal information about an individual’s religion, GPS location, and other personal information that officers can use against the person to stereotype. 92

1. The Eleventh Circuit Disregarded its own Definition of “Intrusiveness” by Failing to Apply it to Electronic Device Border Searches and thus, Violated the Fourth Amendment.

The Eleventh Circuit broadly construes precedent to conclude that both manual and forensic border searches are reasonable without suspicion simply because the search occurs at the border. 93 For example, the Eleventh Circuit uses the holding in United States v. Alfaro-Moncada to justify manual and forensic border searches by concluding that national security interests outweigh a traveler’s right to privacy. 94 The Eleventh Circuit reasons that such searches can prevent issues of national security. 95

Moreover, the Eleventh Circuit justifies the minimization of individual

89. See Riley, 573 U.S. at 395-97 (citing Ontario v. Quon, 560 U.S. 746, 760 (2010)) (noting that today, more than 90% of American adults own cell phones that host mundane and intimate details and records that, until recently, were much more difficult for law enforcement to access).

90. See id. at 395 (comparing a personal diary a decade ago with a cell phone today); United States v. Kolsuz, 890 F.3d 133, 145 (4th Cir. 2018) (explaining that electronic devices contain information such as business documents and medical records).

91. See Kolsuz, 890 F.3d at 145 (noting that electronic devices store uniquely sensitive information that contain intimate details about one’s life).

92. See Riley, 573 U.S. at 395-96 (explaining that apps provide a comprehensive record of a person’s public movements and affiliations that reveal information about a person’s life).

93. See Touset, 890 F.3d at 1228, 1232 (asserting that the border exception has complications because of routine and nonroutine searches and the consequences of each).

94. See United States v. Alfaro-Moncada, 607 F.3d 720, 728 (11th Cir. 2010) (concluding that there is a qualitative balance that exists when the Fourth Amendment is used to balance the international border and the interior of the United States).

95. See id. at 728 (stating that the United States’ paramount responsibility is to protect the sovereign, its territory, and integrity).
privacy rights at the border by emphasizing that a traveler’s desire to enter the United States is a privilege.96 Therefore, travelers should understand that their personal effects, which includes electronic devices, are subject to a forensic search at the border without an officer needing any form of suspicion.97 The Eleventh Circuit unnecessarily overextends the government’s power to conduct forensic searches of an electronic device at the border by asserting that entering the United States is a privilege, but fails to provide any legally sound explanation for not requiring any level of suspicion for searches protected under the Fourth Amendment.98

The Fourth Circuit’s approach creates a norm for officers to conduct manual and forensic searches based on a subjective standard, rather than an objective standard without implicit biases.99 Conducting searches of persons on a subjective basis removes the ability of officers to conduct searches with the objective interest of protecting national security.100 Without a reasonable suspicion standard, permitting an officer to search individuals on a subjective basis creates the risk of the officer using implicit bias to decide which individuals get searched, giving wide discretion to agents at the border.101 For example, an officer can conduct a forensic electronic device search on any traveler at the border, despite being employed in a professional field, not posing a national security risk, and without being in the process of transmitting a crime.102 Thus, the Eleventh Circuit’s legal standard is overly

96. See id. (emphasizing that Fourth Amendment protections are “relaxed” at the border so much so that government officials have the utmost power to reject travelers from entering the U.S. to protect the sovereign (citing United States v. Chemaly, 741 F.2d 1346, 1350 (11th Cir. 1984)).

97. See id. (reiterating that at the border, a person’s personal effects lack protection under the Fourth Amendment).

98. See U.S. CONST. amend. IV (stating, “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”).

99. See Whren v. United States, 517 U.S. 806, 807 (1996) (acknowledging that a law enforcement’s subjective intentions and perspective plays no role in ordinary probable cause search and seizures).

100. See United States v. Kolsuz 890 F.3d 133, 147 (4th Cir. 2018) (noting that forensic searches of electronic devices do not fit within the border search exception and therefore need more than reasonable suspicion. The Riley court acknowledges that forensic border searches need a warrant based on probable cause (citing Riley v. California, 573 U.S. 373, 392 (2014))).

101. See id. at 146 (arguing that Cotterman’s reasoning requires officers to make “commonsense differentiation” between a manual and forensic search, it gives too much discretion to an officer (citing United States v. Cotterman, 709 F.3d 952, 967 (2013))).

broad and goes beyond the border search exception.103

The court asserts that officers can lawfully “pat-down” and “frisk” travelers solely because they request to cross the national border.104 The Eleventh Circuit should expand its rhetoric to include the reasoning in Riley related to electronic device border searches because electronic devices store personal information.105 In Riley, the Supreme Court concluded that searching a cell phone requires probable cause secured by a warrant.106 Instead, however, the Eleventh Circuit relies heavily on Ramsey, noting that CBP agents have reasonable suspicion to search a package when it crosses the border from known sources of illegal activity.107 For example, the Ramsey Court noted that because Thailand was known for heroin distribution in the United States, mail entering the country from Thailand was subject to search without requiring reasonable suspicion.108 However, the Ramsey Court attaches a slightly favorable standard to persons traveling within the United States border.109 It concluded that travelers already in the United States have a right to travel without interruption or search unless there is

search policy goes beyond the scope of the border exception, and completely disregards the impact such a policy has on professionals in professional occupations and their clients’ privileged information).

103. See United States v. Touset, 890 F.3d 1227, 1232 (11th Cir. 2018) (stating the court’s holding that forensic border searches never require suspicion (quoting United States v. Ramsey, 431 U.S. 606, 619 (1977))).

104. See United States v. Alfaro-Moncada, 607 F.3d 720, 728 (11th Cir. 2010) (quoting United States v. Ramos, 645 F.2d 318, 322 (5th Cir. 1981)) (stating that merely crossing the border is enough justification for a traveler to be patted down and frisked, no additional suspicion or cause is needed).

105. See Riley v. California, 573 U.S 373, 395 (2014) (stating that prior to the growth of digital technology, people did not carry sensitive personal information with them on a daily basis).

106. See Touset, 890 F.3d at 1234 (explaining that the Supreme Court has declined to identify the level of suspicion needed to perform a nonroutine search); see also Riley v. California, 573 U.S. at 386 (asserting that a cell phone search requires a level of suspicion because it does not present any sort of Chimel risk).

107. See United States v. Ramsey, 431 U.S. 606, 609-10 (1977) (explaining that the defendant was transporting heroin from Thailand, a country known for mass-producing and transporting heroin into the United States).

108. See id. at 614-15 (explaining that in addition to mail entering from Thailand, there was a statute to confirm the validity of the search; therefore, even if the border search exception did not apply, the search was valid under the statute).

109. See id. at 618 (stating that travelers and their effects outside of the United States border need to prove that they can legally be in the United States and not be a threat to the national security of the country).
probable cause that the traveler is transporting contraband.110

The Eleventh Circuit concludes that its own three-factor test for determining the intrusiveness of a border search, established in Touset, is irrelevant to electronic manual and forensic border searches because both are dissimilar to an x-ray search of a person’s body.111 In conducting a search of an electronic device, officers do not touch the traveler’s body or use physical force to expose the traveler’s body.112 The court incorrectly applied the three-factor intrusiveness test because there was physical contact between Touset and the border officer through his personal effects—the officer touched and searched his luggage and electronic devices.113 Secondly, the test created by Touset is overly vague in that it does not specify what it means to physically expose a traveler’s intimate body parts.114 The vague language of the test, therefore, leads one to argue that an officer is lawfully allowed to expose intimate photographs of a traveler simply by conducting a manual search.115 Specifically, the test allows an officer to scroll through a traveler’s cell phone to view intimate photographs since under the test’s language, the officer is not physically touching the traveler.116

Lastly, the court indicates the use of force as a prerequisite for intrusiveness.117 However, the court fails to acknowledge that the action of force is subjective, difficult to measure, and based on individual factors such as an officer’s physical strength.118 For these reasons, the Eleventh Circuit followed a vague intrusiveness test created by Touset and disregarded that

110. See id. at 620 (noting that what CBP agents really must evaluate is incoming persons and property, not the mode of transportation).
111. See Touset, 890 F.3d at 1234 (listing the three-factors of the court’s intrusiveness test and analyzing how the test does not implicate any violation to the Fourth Amendment).
112. See id. (emphasizing that because the officers in Touset did not physically touch the defendant nor use body strip search methods to search the traveler, no intrusion of privacy occurred).
113. See id. at 1230 (stating that a lookout was issued for Touset’s return to the United States, and when he entered the airport, a CBP agent seized his luggage and searched it).  
114. See id. at 1234 (explaining that the court uses only a body search to define “intrusive” but neglects to consider modern technology).
115. See id. at 1235 (explaining that manual searches have revealed photos of child pornography).
116. See id. (noticing that the court fails to flush through the definition of “physical” and uses it too loosely).
117. See id. 1234 (noting that the court affiliates force with physical strength that can cause harm).
118. See id. (failing to provide a measure of “force”).
both manual and forensic searches of electronics at the border infringe upon an individual’s privacy interests protected under the Fourth Amendment.119

Moreover, even if the Eleventh Circuit’s reliance on the intrusiveness test is valid, the court misapplies the factors of the test for searches conducted at the border.120 Specifically, the court fails to acknowledge what the Supreme Court has already considered in Riley: with the growth of technological advances, travelers no longer keep their personal effects at home.121 Rather, individuals’ private documents are stored and easily accessed on their electronic devices.122 Thus, contrary to the court’s reasoning in Touset, a search of an individual’s electronic device is intrusive under the three-factor test because intrusiveness, force, and touching are subjective to a traveler and a border officer.123

The Eleventh Circuit also uses its precedent to analogize and conclude that an x-ray scan of the body and a forensic search of an electronic device at the border should not be treated the same.124 The court correctly acknowledges that an officer should perform an x-ray scan of a person’s body when reasonable suspicion exists.125 However, using the courts’ intrusiveness test, an x-ray exam does encompass: (1) physical contact between a traveler and an officer; (2) exposure of a traveler’s intimate body parts; and (3) the use of force.126

119. See U.S. CONST. amend. IV (restating the fundamental basis for the Fourth Amendment resides with individual privacy interests to ones’ person and personal effects).

120. See Touset, 890 F.3d at 1234 (stating that the factors of the intrusiveness test are irrelevant to searches of electronic devices because the electronic device is not a physical part of a person).

121. See Riley v. California, 573 U.S. 373, 396-97 (2014) (noting that today, a phone can contain more personal information than a physical house).

122. See United States v. Vergara, 884 F.3d 1309, 1315-16 (11th Cir. 2018) (using the Supreme Court’s rationale that cell phones provide information never found in the home, yet that information has a broad array of private information).

123. See Whren v. United States, 517 U.S. 806, 812-13 (1996) (stating that an officer’s subjective reasoning and intent is irrelevant when determining whether an individual is partaking in criminal behavior).

124. See United States v. Alfaro-Moncada, 607 F.3d 720, 729 (11th Cir. 2010) (describing that an x-ray search of persons’ body requires reasonable suspicion that a crime is being committed or the person and their effects pose a government interest risk).

125. See Touset, 890 F.3d at 1234 (concluding that an x-ray search differs from a forensic search of an electronic device and constitutes a nonroutine search, whereby reasonable suspicion is required).

126. See id. (stating that even at the border, reasonable suspicion is required for highly intrusive searches which include x-rays and strip searches).
Additionally, the Eleventh Circuit incorrectly uses the analogy of an x-ray scan and forensic search of a cell phone. Riley’s rationale concludes that cell phones contain intimate details of one’s life, therefore using sophisticated scanning equipment and software to conduct a forensic electronic device search has the same effect as searching a person’s body with an x-ray machine: both are overly intrusive privacy matters that are inherently protected by the Fourth Amendment. Because the Eleventh Circuit incorrectly categorizes electronic devices as “property” or “effects,” as stated in the Fourth Amendment, the court’s legal standard fails to preserve a traveler’s fundamental right to privacy at the border.

B. The Ninth Circuit’s Interpretation and Application of the Reasonable Suspicion Standard Partially Aligns with the Fourth Amendment’s Protection of Privacy Rights, but should be Expanded to Include an Individualized Suspicion Standard for Electronic Border Searches.

The Ninth Circuit’s legal standard for forensic searches of electronic devices at the border better balances an individual’s privacy rights protected by the Fourth Amendment with the government’s interest in promoting national security. More importantly, the Ninth Circuit acknowledges that there must be limits on the government’s power. However, the Ninth Circuit’s approach to forensic electronic device searches occurring at the border has limitations. Specifically, the court expects travelers to

127. See id. (citing United States v. Montoya de Hernandez, 473 U.S. 532, 541 (1985)) (noting the Court did not decide what level of suspicion is required for a nonroutine border strip search).

128. See Riley v. California, 573 U.S. 373, 397 (2014) (explaining that the privacy interest of searching a cell phone not only exposes the data a user regularly accesses but data that might not be stored on the device itself. For example, the traveler can have their cell phone synced to a Cloud storage in a different location and still access more information that is not stored on the cell phone itself).

129. See id. at 384 (referencing precedent that shows a person’s personal property includes things immediately near him during a search).

130. See United States v. Cotterman, 709 F.3d 952, 960 (9th Cir. 2013) (explaining that it is fundamental for the court to draw a clear distinction between government interests and individual privacy interests. The Government cannot be allowed to unjustly seize property for extended times without justification to be used as criminal evidence against an individual crossing the border).

131. See id. at 957 (stating that even though the government cannot be required to have equipment readily available at the border to conduct forensic searches of electronic devices, the government cannot simply practice an “anything goes” process).

132. See id. at 961 (explaining that an “extended” border search, commonly known as a forensic search, is only permissible when it is apparent with reasonable certainty that
understand that forensic searches of electronic devices can occur hundreds of miles away from the border.133 This expectation unrealistically forces travelers to inform themselves that their electronic devices are subject to a forensic search even at a distance that is far from the border.134 Even though the Ninth Circuit makes an effort in considering a traveler’s privacy rights, it falls short by failing to establish a legal standard that objectively considers who should be subjected to a forensic search.135

The Ninth Circuit’s legal standard for lawfully conducting forensic searches of electronic devices at the border is based on reasonable suspicion and is a two-pronged test.136 First, for a forensic electronic device search to be lawful, the traveler must have recently crossed the border, and second, the officer must have reasonable suspicion that criminal activity has occurred or will occur.137 Similarly to the Eleventh Circuit, the legal question raised by the Ninth Circuit’s legal standard is that it still favors a subjective approach to conducting forensic electronic device searches.138 The Ninth Circuit moves closer to a balanced standard for conducting forensic searches of electronic devices at the border.139 In particular, the Ninth Circuit reasons

---

133. See id. at 960 (clarifying that the court’s expectation exists because according to the traditional interpretation of the border search exception, an individual loses their privacy protection at the border).

134. See id. at 974-75 (asserting that the border search exception is not rigid and there should not be an expectation for the United States to have forensic search equipment readily available at each port-of-entry or border).

135. See Riley v. California, 573 U.S. 373, 403 (2014) (noting that cell phones are not immune from search, but a warrant is generally required even when the search occurs incident to arrest. The Court also emphasizes that cell phones are not just technological conveniences, they hold “the privacies of life”).

136. See Cotterman, 709 F.3d 961 (citing United States v. Guzman-Padilla, 573 F.3d 865, 878-79 (9th Cir. 2009)) (explaining the dual requirements and their establishment to protect government interests).

137. See id. (explaining their legal standard and the overarching objective: conforming to government needs, concluding that the sovereign does not need to make any special justifications to search at the border).

138. See United States v. Touset, 890 F.3d 1227, 1234 (11th Cir. 2018) (noting that the Fourth Circuit and Ninth Circuit both agree that reasonable suspicion is required for “extended” forensic searches of electronic devices at the border).

139. See Cotterman, 709 F.3d at 960 (citing United States v. Montoya de Hernandez, 473 U.S. 531, 539 (1985)) (concluding that the government does not have carte blanche at the border; therefore, the Fourth Amendment protections do not disappear at the border).
that when a traveler’s electronic device is destroyed during or before a forensic search, CBP agents must have reasonable suspicion before initiating the search.140

While the Ninth and Eleventh Circuits have similar interpretations of the border search exception, the Ninth Circuit properly holds that border searches of forensic electronic devices, without reasonable suspicion, are an intrusion on an individual’s protected privacy rights.141 Moreover, although only relevant until after the subject or items have entered the U.S., the Ninth Circuit’s legal standard addresses not only the type of search but the distance where the search is conducted.142 The Ninth Circuit’s legal standard asserts that a person’s expectation of privacy does not cease at the border or its functional equivalent.143 Therefore, when the government conducts an extended search, inherently delayed in nature and extending beyond the actual border, it must justify the search with reasonable suspicion.144

The Ninth Circuit erred by disagreeing with the district court’s conclusion that a traveler cannot be subject to a forensic electronic device search, if while at the border, the government had no evidence of criminal acts in transit.145 Rather, to forensically search and seize a traveler’s electronic device, the government should have evidence, such as through a lookout

140. See id. at 962-63 (explaining that proximity to the border is just one factor the court considers when enforcing the border search exception); see also United States v. Villasenor 608 F.3d 467, 471-72 (declining to enforce the border search exception within a few miles of the border).

141. See Cotterman, 952 F.3d at 957 (noting the intrusive nature of forensic examinations and its Fourth Amendment implications. Moreover, the Fourth Amendment asserts its privacy protection against intrusion when a search is conducted beyond the border, where a traveler’s normal expectation of privacy is attached).

142. See id. at 962-63 (emphasizing that a heightened level of suspicion should arise when forensic searches of an electronic device occur away from the border or at the border’s “functional equivalent,” which can extend hundreds and even thousands of miles away from the physical border).

143. See id. at 962 (citing United States v. Cotterman, 637 F.3d 1068, 1086-87 (9th Cir. 2011) (Fletcher, J. dissenting)) (explaining that seizure of a person or their belongings does not become unreasonable because the seizure is extended in time. However, what really matters is the scope of their detention. The court must find that the detention remains related to the initial search and seizure).

144. See United States v. Abbouachi, 502 F.3d 850, 855 (9th Cir. 2007) (explaining that extended searches go beyond the regular expected border search, thus requiring a particularized level of suspicion to uncover contraband or evidence of criminal activity).

145. See Cotterman, 637 F.3d at 1074 (explaining that the United States argued that if the border officer’s initial search was based on reasonable suspicion, the officer no longer has to justify an extended forensic border search because the original finding of suspicion is transferred).
According to the Ninth Circuit, it is not necessary to dwell on the government’s border search power because the First Congress’s rationale for the Fourth Amendment has historically taken precedent: customs border agents could conduct warrantless searches of vessels crossing the border for contraband. However, the Ninth Circuit incorrectly holds in Cotterman that a traveler’s presence at the border automatically foregoes his Fourth Amendment protections. The court’s holding is incorrect because a traveler’s right to privacy is not diminished the instant he presents himself at the border. Rather, being at the border should alert a traveler that his right to privacy is less applicable, but never completely removed, because as the court asserts, the government cannot seize property for weeks to conduct a forensic search without first having reasonable suspicion. Interestingly, the Ninth Circuit’s reasoning seems to contradict itself: first it asserts that a traveler’s Fourth Amendment protection is waived at the border, but later asserts that forensic searches require reasonable suspicion based on the totality of the circumstances in each case. Its reasoning must be more

146. See id. (restating the District Court’s ruling: The United States does not dispute that there was insufficient evidence to conduct a forensic search of the electronic devices 170 miles away from the border).

147. See United States v. Ramsey, 431 U.S. 606, 616-18 (1977) (providing an explanation of the First Congress’s interpretation of the Fourth Amendment: Section 24 authorizes custom and border officers to lawfully enter and search dwellings of crewmembers on vessels); see also Cotterman, 637 F.3d at 1074 (stating that because ICE agents relayed information that seemed to incriminate the defendant, the government was allowed to conduct a forensic search of an electronic device without considering whether they actually had evidence that established reasonable suspicion).

148. See Cotterman, 637 F.3d at 1078 (concluding that the border search exception still applies to searches initiated at the border with devices that have not been cleared to enter the United States. The court contends that the border search exception allows a search to continue beyond the border to determine whether the device causes a risk to the sovereign).

149. See United States v. Kolsuz, 890 F.3d 133, 145 (4th Cir. 2018) (citing Riley v. California, 573 U.S. 373, 403 (2014)) (stating that Riley presented the notion that a cell phone should not be treated as just another form of a container, rather, cell phones are different: they impose a risk to expose sensitive information without probable cause).

150. See Cotterman, 637 F.3d at 1070, 1077 (claiming that if a traveler’s initial search occurs at the border, that traveler no longer has a “normal” expectation of privacy. However, a line must be drawn: the Government cannot seize property at the border and hold it for weeks, months, or years on a whim).

151. See id. at 1079 (quoting the court: “We continue to analyze the Government’s conduct on a case-by-cases basis” to determine when a search is unreasonable; the reasoning should be based on the duration and scope of the search).
uniform. 152 Through this rationale, the Ninth Circuit, similar to the Eleventh Circuit, entirely disregards the Fourth Amendment’s inherent protection against unreasonable intrusion. 153

Cotterman, like many other travelers crossing the border, did not expect the government to conduct a forensic electronic search of his device away from the border without having individualized suspicion. 154 This expectation is reasonable because the traveler has no direct knowledge of when the search will cease or what the government is actually looking for. 155 Cotterman’s argument is persuasive because it exemplifies a common concern for travelers: travelers should not be expected to leave their personal effects and electronic devices at home to prevent being subject to such an intrusive search. 156


The individualized suspicion standard that the Fourth Circuit applies to forensic electronic device searches at the border is the correct standard

152. See id. (providing examples of the court’s reasoning being unclear).
153. See United States v. Vergara, 884 F.3d 1309, 1310 (11th Cir. 2018) (concluding that the two requirements under the Fourth Amendment to search and seize, probable cause and a warrant, are never required at the border unless it is an x-ray examination or strip search); see also United States v. Touset, 890 F.3d 1227, 1229 (11th Cir. 2018) (reiterating that reasonable suspicion is not required for initial search of an electronic device at the border; therefore, no suspicion is needed to search electronic devices at the border regardless if the search is manual or forensic); Cotterman, 709 F.3d at 967 (concluding that travelers should expect to have their privacy intruded upon during a border search).
154. See Cotterman, 637 F.3d at 1076 (reiterating that under the border search exception, the government can conduct searches of property away from the border not yet cleared for entry).
155. See id. at 1074 (referencing Cotterman’s argument that the border search exception is ambiguous and allows the government to conduct forensic searches of electronic devices without sufficient evidence and can lead to extended border searches without particularized suspicion).
156. See United States v. Kolsuz, 890 F.3d 133, 145 (4th Cir. 2018) (emphasizing that electronic devices are found everywhere and used by everyone regardless of being a criminal or law-abiding citizen. In addition, electronic devices are the most efficient tools used for communication when a traveler is abroad, and it is unreasonable and unrealistic to ask a traveler to leave his electronic devices at home because of the border search exception); Contra United States v. Thirty-Seven Photographs, 402 U.S. 363, 376 (1971) (concluding that a person should not have the same expectation of privacy at a port as they do their home).
because it aligns and complies with the inherent privacy protections guaranteed in the Fourth Amendment.\textsuperscript{157} In \textit{Kolsuz}, the Fourth Circuit did not address or resolve the level of suspicion needed in the course of a manual electronic device search at the border.\textsuperscript{158} Instead, the court uses \textit{Kolsuz} to address whether more than reasonable suspicion is needed to conduct forensic electronic device searches at the border.\textsuperscript{159} However, since the Fourth Circuit is the only circuit that suggests that a higher level of reasonable suspicion is needed to conduct a forensic search at the border, the Fourth Circuit should consider addressing manual searches in future cases.\textsuperscript{160} The Fourth Circuit’s determination that individualized suspicion is needed to conduct forensic searches of electronic devices at the border serves the Congressional intent of prioritizing government interests and protecting an individual’s right to privacy that the Fourth Amendment guarantees.\textsuperscript{161} For example, on two separate occasions prior to the forensic search of Kolsuz’s electronic devices, CBP agents found illegal firearm parts in his luggage and reminded him that he needed a license to transport the parts; he did not comply.\textsuperscript{162} In 2016, CBP agents received a registered alert listing prior border searches revealing Kolsuz’s same illegal transport of firearm parts, establishing individualized suspicion, and leading to two suitcases full of contraband.\textsuperscript{163} The Fourth Circuit’s legal standard is compliant with the

\begin{itemize}
  \item \textsuperscript{157} \textit{See Kolsuz}, 890 F.3d at 135 (concluding that a traveler’s right to privacy does not stop at the border. Rather, the government is required to have specific reasons to conduct a forensic search of an electronic device based on individualized suspicion).
  \item \textsuperscript{158} \textit{See id.} at 141 (using the fact that Kolsuz did not dispute the manual search of his electronic device at the border to justify their reasoning for not addressing manual searches of electronic devices at the border).
  \item \textsuperscript{159} \textit{See id.} at 142 (suggesting that Kolsuz does not dispute the manual search because he was arrested during the forensic search, which uncovered more private information on his cell phone; whereas the manual search at the airport did not reveal information used against him at trial).
  \item \textsuperscript{160} \textit{See id.} at 140 (stating that \textit{Riley} helps to acknowledge that electronic devices serve as property, and therefore are protected by the Fourth Amendment).
  \item \textsuperscript{161} \textit{See United States v. Touset}, 890 F.3d 1227, 1236 (11th Cir. 2018) (acknowledging the Congressional intent of the border search exception: officers are required to have reason to suspect contraband is being imported); \textit{See Kolsuz}, 890 F.3d at 137 (agreeing with \textit{Riley}: forensically searching an electronic device requires more than reasonable suspicion).
  \item \textsuperscript{162} \textit{See Kolsuz}, 890 F.3d at 141 (explaining that Kolsuz did not contest or reject the fact that his electronic devices were seized, he also had prior knowledge of the licensing requirements to transport such fire arm parts and never complied).
  \item \textsuperscript{163} \textit{See id.} at 143 (explaining that CBP agents rightfully forensically searched Kolsuz’s phone because they had good reason (his history) to believe that he would continue transporting illegal fire arm parts).
\end{itemize}
Fourth Amendment because a forensic search of electronic devices requires the government to produce a greater justification for conducting the search.164 In *Kolsuz*, the court applied an individualized suspicion standard and thereby correctly rejected the defendant’s argument against the forensic search.165 Kolsuz argued that because he was exiting the United States, the border search exception did not apply, but he is incorrect.166 Moreover, Kolsuz’s continuous efforts to transport illegal weapon-parts speaks directly to the basis of the border search exception which aims to prevent dangerous contraband from entering the United States.167 In hindsight, the Fourth Circuit recognizes that even at the border, the government’s authority is limited because electronic device searches must be subject to reasonableness.168 The Fourth Circuit’s legal standard is an example of an objective legal standard that correctly balances both government and personal interests because it acknowledges that a forensic search at the border reveals sensitive and private information.169 In addition, the Fourth Circuit relies on precedent that acknowledges cell phone searches go beyond the normal expected standard of intrusion.170 In 2012, CBP agents discovered 163 illegal firearms in Kolsuz’s luggage; the firearms were added to the United States Munitions List (hereinafter “USML”).171 To add a

164. *See id.* (agreeing with the District Court’s holding but adding that perhaps there must be a higher warrant-based rule for nonroutine searches of electronic devices at the border, suggesting that maybe a warrant-based standard should be developed).

165. *See id.* at 138 (describing the long history of the defendant’s criminal activity. When the defendant attempted to exit the United States, he was already “well known” to government authorities for exporting fire arm parts without an export license).

166. *See id.* (asserting the basis of the border search exception is to protect against national security risks, which give way to regulating imports and exports).

167. *See id.* (explaining that the purpose of the border search exception is to monitor the transport of dangerous weapons).

168. *See id.* (emphasizing that the touchstone of the Fourth Amendment is reasonableness to search and seize).

169. *See id.* at 140 (explaining that a manual search of an electronic device requires no level of suspicion because such a search is implied for travelers entering and existing the border. However, a forensic search, whereby a cell phone is seized from its owner, connected to a sophisticated piece of equipment which is developed to analyze and extract data beyond a manual search, can no longer be compared to an ordinary search of ones’ luggage).

170. *See id.* (stating that Supreme Court precedent has acknowledged the difficulties in categorizing a forensic search of a cell phone as just a manual search; instead, the Court concluded that such a search is easily comparable to a “body cavity search” of a phone).

171. *See id.* at 138 (explaining that under the Arms Export Control Act, firearm parts are considered defense articles subject to licensing requirements).
weapon to the USML, the government must have a justified reason that the weapon itself is a national security risk. The Fourth Circuit’s legal standard for forensic searches complies with the Fourth Amendment because it requires border officials to have specific reasons to conduct such a search, like the defendant’s long history of transporting illegal contraband. Additionally, following Kolsuz’s arrest, the forensic search of his cell phone revealed information showing that he intended to continue transporting illegal firearms. Moreover, without a legal standard based on individualized suspicion, CBP agents are searching travelers based on a subjective standard. Having a legal standard based on individualized suspicion prevents the government from having free rein to unequivocally forensically search without reason. In turn, this will produce an interest-balanced standard that reduces Fourth Amendment violation claims of “unreasonable search or seizure.”

In Kolsuz, the Fourth Circuit agreed with the Ninth Circuit’s holding that after an electronic device search is initiated at the border, proximity is no longer an issue. The Fourth Circuit has also taken an approach that respects governmental interest, an individual’s right to privacy, and its

172. See id. at 139 (explaining that once a weapon is added to the United States Munitions List, it cannot be removed from the United States without a license).

173. See id. at 138 (describing the long list of encounters and warning border officers had with the defendant prior to the forensic search of his electronic devices. The encounters occurred for a number of years).

174. See id. at 143 (providing the explanation that the forensic search showed ongoing efforts to continue transporting illegal firearms to Miami and Turkey from the United States).

175. See United States v. Touset, 890 F.3d 1227, 1232 (11th Cir. 2018) (asserting that there is no need for an extended legal standard to incorporate specific reasons to conduct a forensic search).

176. See Kolsuz, 890 F.3d at 135 (explaining that there needs to be a balanced objective standard for Fourth Amendment exceptions. Moreover, when an individual’s privacy interests outweigh government interests, a warrant based on probable cause is required).

177. See id. at 141 (citing United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985)) (explaining that courts have justified the most intrusive nonroutine searches with reasonable suspicion, including the case where the Court used an x-ray to ensure that a suspect was smuggling drugs, and detained the criminal until the drugs was excreted from her alimentary canal).

178. See id. at 142 (citing United States v. Cotterman, 709 F.3d 952, 961-62 (2013)) (concluding once an electronic device search started at the border, conducting an off-site forensic search away from the actual border is permissible and does not remove the border exception).
extension to property, including electronic devices. The Fourth Circuit’s legal standard is in line with the Fourth Amendment’s privacy protection because it requires the government to demonstrate significant proof that an individual is in transit to commit a crime before being able to conduct a forensic search.

The interesting nuance between the circuit courts is that all suggest that the legislative and executive branches of government further examine the issue and implications of electronic device searches at the border. They recommend that Congress use its law-making power to create an objective standard to determine the level of suspicion required for border searches.

By adopting the Fourth Circuit’s rationale, circuit courts will be able to properly apply Riley’s individualized suspicion standard instead of applying a reasonable suspicion standard, or failing to apply a standard at all when performing nonroutine-forensic electronic device searches at the border. A standard based on individualized suspicion is more effective; it serves as a safeguard for travelers and allows CBP agents to properly investigate actual risks to national security based on individual suspicion, rather than subjective beliefs. An individualized suspicion standard ensures that the individual subjected to the search is guaranteed protection over his private interests, such as his political affiliations, religious views, location, and

179. See id. at 143 (explaining that when a Fourth Amendment search exception is applicable and there are ancillary governmental interests, the court must enforce the paramount protection described in the Fourth Amendment, the government must obtain a warrant based on probable cause).

180. See id. (explaining that CBP agents found two suitcases of firearm parts and did not just search Kolsuz’s belongings to invoke the border exception to generalized law enforcement interests and combating crime).

181. See id. at 148 (Wilkinson, J., concurring) (emphasizing that different standards of suspicion should be determined by Congress and courts should apply it. In addition, because border searches of electronic devices are becoming more common, all three branches of government need to approach the topic, not just one).

182. See id. at 148 (emphasizing that the legislative and executive branches of government have a critical role in defining the standard for border searches and therefore, are better equipped to create rules that govern individual privacy rights and governmental interests).

183. See Riley v. California, 573 U.S. 373, 374 (2014) (emphasizing that a search of a cell phone does not further the government interests in Chimel but has a greater privacy interest than a brief physical search).

184. See id. at 394 (explaining the justification for expanding the standard of suspicion for cell phone searches: a cell phones’ storage capacity has consequences that raise several privacy concerns. A cell phone collects and stores information such as personal contacts, addresses, financial and medical records, and thousands of photographs that show a person’s private life).
browsing history.\textsuperscript{185} Moreover, manual routine searches are already exempted from the standard Fourth Amendment requirements: probable cause and a warrant; therefore, CBP agents are free to assess risks concerning national security and safety without having to forensically search an electronic device.\textsuperscript{186}

Having courts recognize the importance of individualized suspicion is useful but not enough.\textsuperscript{187} The inconsistencies between circuit courts regarding forensic electronic device searches directly infringe on the primary purpose of the Fourth Amendment: to protect against government intrusion.\textsuperscript{188} As a result, it becomes cumbersome and difficult for travelers and law enforcement officers to understand when to proceed with such a search.\textsuperscript{189} Furthermore, because the Fourth Circuit, like its sister circuits, chose not to address manual searches, the individualized suspicion standard is still vague because no standard objective test exists for border officials to use.\textsuperscript{190} Therefore, any search can be considered manual or forensic.\textsuperscript{191} Moreover, the concurring opinion in \textit{Kolsuz} emphasizes the need to resolve empirical questions that will help create an objective legal standard

\begin{flushleft}
185. See \textit{id.} at 396 (citing Justice Sotomayor’s point of view: cell phones contain particularized information that is meant to be kept private).

186. See \textit{Kolsuz}, 890 F.3d at 135 (explaining that the Fourth Amendment is broad enough to prevent contraband without having to forensically search when individualized suspicion is absent).

187. See \textit{id.} at 133 (referring to circuit cases that disagree on the legal standard of the border search exception).

188. See generally United States v. Touset, 890 F.3d 1227 (11th Cir. 2018), \textit{Kolsuz}, 890 F.3d at 133, United States v. Cotterman, 637 F.3d 1068 (9th Cir. 2011) (citing the circuit court cases that differ on the standard of suspicion needed to conduct a forensic electronic device search at the border or its functional equivalent).

189. See \textit{Kolsuz}, 890 F.3d at 148 (Wilkinson, J., concurring)(noting that if, as the majority declares, individualized suspicion is required to conduct a forensic search of an electronic at the border, then Congress must say so. Moreover, issues like border searches are the reason why the government must be active in the separation of powers; all branches of government must participate in such a policy, “not just one”).

190. See \textit{id.} at 146 (explaining that at this point, even though CBP implemented the \textit{Border Search of Electronic Devices} directive, it does not establish a constitutional mandate).

191. See \textit{id.} at 148-49 (noting that even though the majority chose not to address manual searches at the border, individualized suspicion can apply to manual searches as well. Moreover, the majority should have found that the forensic search was reasonable, rather than allowing the distinction of intrusive and less intrusive be the deciding factor in whether or not individualized suspicion was present because such distinction allows for slipperiness).
\end{flushleft}
minimizing tension between privacy and security interest at the border.\footnote{192}{See id. at 150 (stating specific questions that are critical to answer in order to establish an objective legal standard).}

### IV. Policy Recommendations

With the advance of modern technology and the new administration, electronic device searches at the border have increased to almost 15,000 in the first half of 2017, and is estimated to triple at the end 2017.\footnote{193}{See American Civil Liberties Union, Alasaad v. Nielsen: Challenge to Warrantless Phone and Laptop Searches at U.S. Border, THE AMERICAN CIVIL LIBERTIES UNION (Nov. 17, 2018, 12:47 AM), https://www.aclu.org/cases/alasaad-v-nielsen-challenge-warrantless-phone-and-laptop-searches-us-border (addressing the recent trend of border searches of electronic devices and its effect on professionals who cross the border).} The border search exception’s purpose is to protect the sovereign from national security risks, yet it is proven that the exception encroaches upon, and on occasion can violate an individual’s privacy interest.\footnote{194}{See Riley v. California, 573 U.S. 373, 386 (2014) (acknowledging that cell phones differ from other physical objects because they store an immense amount of information that is readily available upon a warrantless search).} Courts drastically vary with their interpretations of the border search exception and need an objective legal standard to evaluate cases based on the border search exception.\footnote{195}{See generally United States v. Touset, 890 F.3d 1227, 1229 (11th Cir. 2018), Kolsuz, 890 F.3d at 133, United States v. Cotterman, 637 F.3d 1068, 1070 (9th Cir. 2011) (showing how each circuit court applied the border search exception to forensic searches of electronic devices differently).} In deciding what an objective legal standard would be, the legislative branch should utilize the Fourth Circuit’s standard for forensic searches and incorporate the Eleventh Circuit’s three-factor intrusiveness analysis.\footnote{196}{See Riley v. California, 573 U.S. 373, 408 (2014) (Alito, J., concurring) (stating that with the growth of modern day technology, it would be “very unfortunate” if in the twenty-first century, privacy protection of electronic devices was left for the federal courts to analyze using only the “blunt” instrument of the Fourth Amendment. Noting that the legislative branch is in a better place to determine a standard, objective assessment to handle electronic device border searches); see also Kolsuz, 890 F.3d at 150 (agreeing with the suggestion that the legislative and executive branches of government are better equipped to create a standard test because they are elected by the people).} Moreover, the legislative branch should strictly review this exception and objectively create a standard for manual and forensic searches.\footnote{197}{See Kolsuz, 890 F.3d at 149 (Wilkinson, J., concurring) (emphasizing that the only responsibility of the judicial branch is to apply the law to the facts of the case; to do so, the legislative and executive branches must use their power to create an objective standard).}
Reasonable suspicion is the appropriate standard for manual border searches because, while CBP agents are entrusted to protect government interests, they should only initiate a manual search when they are notified that a traveler is a suspect to a crime or is in the process of committing a crime. Additionally, for a forensic electronic device search, the standard of suspicion should be individualized suspicion, based on specific facts.

The overly broad language of DHS’s electronic device border search policy allows the government to overextend their power, hence the difficulty for circuit courts to agree on when, how, and why a traveler’s electronic devices are subject to a manual or forensic border search. This kind of inconsistent policy creates an environment where travelers and law enforcement officers argue against one another and their prospective privacy interests.

Factors such as: whether a traveler has a history of criminal behavior, the kind of criminal charges, the type of electronic device, and the ways in which officers conduct the search, are fundamental questions that help to create an objective standard. Moreover, the correct legal standard for manual searches of electronic devices is reasonable suspicion and individualized suspicion for forensic searches of electronic devices at the border.

---

198. See id. at 139 (noting that even a manual search of an electronic device can be intrusive: a manual search involves using the iPhone’s touch screen feature to scroll through recent calls and text messages).

199. See id. at 133 (stating that extended border searches are nonroutine searches, thus requiring the individual to be subjected to more personal intrusion of their private effect; such a search requires individualized suspicion); see also Cotterman, 637 F.3d at 1079 (referencing Supreme Court precedent to establish that the manner in which an initial border search is conducted may require a heightened degree of suspicion, whereby even an initial search can be unreasonable).

200. See Touset, 890 F.3d at 1229 (concluding that searches of electronic devices at the border never require probable cause or a warrant. Moreover, no suspicion is required to search electronic devices at the border, regardless of the search being manual or forensic); Kolsuz, 890 F.3d at 133 (concluding that individualized suspicion is required to forensically search an electronic device at the border); Cotterman, 709 F.3d at 968 (concluding that reasonable suspicion is needed to conduct a forensic search of an electronic device at the border).

201. See Kolsuz, 890 F.3d at 148 (Wilkinson, J., concurring) (acknowledging the importance of having a third governmental branch, the Legislature, create a rule that is objective for the courts to apply).

202. See Touset, 890 F.3d at 1234 (using Touset to inspire a standardized, objective test).

203. See Kolsuz, 890 F.3d at 135 (asserting that nonroutine searches deeply intrude on a person’s privacy, thus requiring individualized suspicion); see also Riley v. California, 573 U.S. 373, 403 (2014) (emphasizing that today, technology allows an
CONCLUSION

A Fourth Amendment exception that does not have an objective legal standard to assess whether a constitutional violation has occurred is useless to the judiciary branch and gambles with government and individual privacy interests.204 An objective legal standard should not give the government an individual preference, rather it should limit power discretion between both parties and formulate a test whereby any court can effectively apply factors that result in an unbiased showing of the facts and the law.205 The Fourth Circuit attempts to create an objective standard test for forensic searches of electronic devices by concluding that individualized suspicion is needed for such a search; however, this standard must be established through the legislative body.206

individual to carry personal information by hand and does not allow for a lesser protection of privacy; a warrant is still generally required and obtaining a warrant is also easier for law enforcement because they can receive warrants electronically).

204. See Kolsuz, 890 F.3d at 137 (explaining the importance of having a different level of suspicion when conducting an electronic device search at the border); see United States v. Cotterman, 637 F.3d 1068, 1079-80 (9th Cir. 2011) (explaining three different types of border searches and the level of suspicion needed to search).

205. See Riley, 573 U.S. at 407-088 (Alito, J., concurring) and Kolsuz, 890 F.3d at 148 (Wilkinson, J., concurring) (emphasizing the need for the legislative and executive branch to step-in and produce a law that evaluates the border search exception).

206. See Kolsuz, 890 F.3d at 149 (noting that if an objective standardized test is created by federal courts, there will be a slippery slope ahead).