Akron Law Review

Volume 53
Issue 3 *Federal Appellate Issue*

Article 7

2019

Forensic Searches of Electronic Devices and the Border Search Exception: Movement Toward Requirement for Particularized Suspicion

Marissa Pursel

FORENSIC SEARCHES OF ELECTRONIC DEVICES AND THE BORDER SEARCH EXCEPTION: MOVEMENT TOWARD A REQUIREMENT FOR PARTICULARIZED SUSPICION

*Marissa Pursel**

I. INTRODUCTION

In the interest of national security, travelers are often required to endure some degree of inconvenience, delay, and invasion of personal privacy. Prior to boarding any commercial flight, for example, individuals are frequently asked to comply with certain rules and undergo security screenings.[1] Many of us have experienced passing through airport security where a stoic TSA agent asked us to remove our shoes, place our personal belongings on a conveyor belt to be screened, and walk through the metal detectors.[2] These policies and procedures are even stricter in the context of international travel—all travelers are subject to examination and search by Customs and Border Protection (CBP).[3] While it can certainly feel burdensome, most travelers understand that heightened security measures at the airport are a small price to pay for a safer America, especially in light of the September 11, 2001 terrorist attacks.[4] But at what point does mere inconvenience become a significant invasion of privacy that travelers no longer anticipate?

The Fourth Amendment guarantees to American citizens a constitutional right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[5] It is important to note that the Fourth Amendment does not prohibit *all* searches and seizures—only those which are unreasonable violate the U.S.

---

* Marissa Pursel is a J.D. Candidate, 2020, University of Akron School of Law. Many thanks to Randolph Baxter Professor of Law Martin Belsky for his expertise and thoughtful guidance in the writing of this article, and to the entire *Akron Law Review* staff. Thank you as well to my family and friends who have patiently supported me throughout the writing process.

1. At the airport, the Transportation Security Administration (TSA) screens travelers' carry-on bags for "explosives and other dangerous items." TSA workers also request that travelers remove their larger electronic devices such as laptops from their carry-on bags for x-ray screening. Under certain circumstances, travelers may be required to undergo a pat-down search. *Security Screening*, TRANSPORTATION SECURITY ADMINISTRATION, https://www.tsa.gov/travel/security-screening [https://perma.cc/73S7-QALE].

2. *Id.*

3. *CBP Search Authority*, U.S. CUSTOMS AND BORDER PROTECTION, https://www.cbp.gov/travel/cbp-search-authority [https://perma.cc/42KS-RQVL].

4. Following September 11, 2001, the U.S. has placed greater focus on national security and law enforcement in an effort to "apprehend potential perpetrators and prevent future tragedies." John M. Allen, Note, *Expanding Law Enforcement Discretion: How the Supreme Court's Post-September 11th Decisions Reflect Necessary Prudence*, 41 SUFFOLK U. L. REV. 587, 590 (2008).

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

Constitution.[6] Generally, a "reasonable" search is one that is conducted pursuant to a warrant issued upon a finding of probable cause.[7] Thus, "searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."[8] For example, the government may conduct a warrantless search where an individual is lawfully arrested,[9] voluntarily consents to the search,[10] or seeks entry to or exit from the United States.[11]

Where a search is conducted at the border rather than within the United States, the Fourth Amendment's "reasonableness" requirement is quite different.[12] Pursuant to the border search exception, the government may search travelers and their belongings at the border without showing probable cause and without first obtaining a warrant.[13] As a general rule, searches at the border do not even require reasonable suspicion, provided the search is "routine."[14] The rationale for the border search exception rests on the government's interest in national security, and searches at the border are deemed reasonable "simply by virtue of the fact that they occur at the border."[15]

Electronic devices have created uncertainty in the context of the border search doctrine.[16] In determining whether searches of electronic devices at the border require any degree of particularized suspicion, courts have begun to consider whether a distinction should be made between various types of travelers' property.[17] Arguably, a meaningful distinction should be made between classes of property subject to search at the

6. Terry v. Ohio, 392 U.S. 1, 9 (1968) (citing Elkins v. U.S., 364 U.S. 206, 222 (1960)).

7. Benjamin J. Rankin, Note, *Restoring Privacy at the Border: Extending the Reasonable Suspicion Standard for Laptop Border Searches*, 43 COLUM. HUM. RTS. L. REV. 301, 301 (2011).

8. Katz v. United States, 389 U.S. 347, 357 (1967).

9. Arizona v. Gant, 556 U.S. 332, 338 (2009).

10. Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

11. Jon Adams, *Rights at United States Borders*, 19 BYU J. PUB. L. 353, 354–55 (2005).

12. *Id.* at 355 (noting that "in view of Congress' power to regulate international commerce, the Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior.").

13. Sunil Bector, *"Your Laptop, Please:" The Search & Seizure of Electronic Devices at the United States Border*, 24 BERKELEY TECH. L.J. 695, 697 (2009).

14. Adams, *supra* note 11, at 354.

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

16. Thomas Mann Miller, Comment, *Digital Border Searches After Riley v. California*, 90 WASH. L. REV. 1943, 1945 (2015) (arguing that federal courts have had the "difficult task" of determining how the Supreme Court's decisions in the area of border searches, which thus far have only addressed searches of persons and items of tangible property, should be applied to searches of electronic devices).

17. *See, e.g.*, United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013); United States v. Kolsuz, 890 F.3d 133 (4th Cir. 2018); United States v. Touset, 890 F.3d 1227 (11th Cir. 2018).

border; electronic devices, which contain a vast amount of sensitive personal information, are fundamentally and substantively distinguishable from the ordinary luggage traditionally subject to manual search.[18] While it is well established that the federal government has "plenary authority" to conduct "routine" searches at the border without a showing of any particularized suspicion,[19] forensic searches of electronic devices should be subject to a higher standard.[20]

A pair of 2018 decisions in the Circuit Courts, decided only 14 days apart, highlight the issue of forensic searches of electronic devices at the national border.[21] In *Kolsuz*, a traveler was detained at an international airport after border agents found firearm parts in his luggage, which Kolsuz lacked the appropriate license to transport.[22] The agents confiscated Kolsuz's smartphone and conducted an extensive forensic examination, extracting almost 900 pages of digital information.[23] The Fourth Circuit found the off-site forensic search to be nonroutine, but this finding was not outcome-determinative—the evidence was properly admitted upon a finding that the officers had reasonable suspicion to perform the search.[24]

Two weeks later, the Eleventh Circuit refused to recognize any distinction between searches of electronic devices and the traditional routine searches conducted at the border, finding forensic searches themselves to be routine.[25] In *Touset*, a traveler suspected of possessing and distributing child pornography was stopped at an international airport where border agents confiscated his cell phones, camera, tablets, and external hard drives.[26] Forensic searches were performed on several

18. Tom Rechtin, *Back to the Future of Your Laptop: How Backlash over Prolonged Detention of Digital Devices in Border Searches is Symptomatic of a Need for "Reasonable Suspicion" in All Border Searches of Digital Devices*, 7 IDAHO CRITICAL LEGAL STUD. J. 65, 87 (2014) (suggesting that "it would be inappropriate to apply a set standard for all property" because "not all pieces of personal property possess the same kind of relation to the person who owns them.").

19. United States v. Montoya De Hernandez, 473 U.S. 531, 537 (1985).

20. *See Cotterman*, 709 F.3d at 966 (holding that reasonable suspicion should be required for forensic searches of computers, recognizing "the uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy and thus renders an exhaustive exploratory search more intrusive than with other forms of property."). More recently, the Fourth Circuit found a forensic search of a traveler's electronic device to be "nonroutine" and "permissible only on a showing of individualized suspicion." *See Kolsuz*, 890 F.3d at 144.

21. *See* United States v. Kolsuz, 890 F.3d 133 (4th Cir. 2018); United States v. Touset, 890 F.3d 1227 (11th Cir. 2018).

22. *Kolsuz*, 890 F.3d at 136.

23. *Id.* at 139.

24. *Id.* at 136–37.

25. *Touset*, 890 F.3d at 1233.

26. *Id.* at 1230.

devices, revealing child pornography.[27] Although the Eleventh Circuit held that no reasonable suspicion was required to conduct the forensic search, this finding was not outcome-determinative as customs agents had reasonable suspicion prior to the search.[28]

Forensic searches are unique—digital devices are capable of housing exponentially more information than a suitcase could ever hold.[29] Moreover, electronic devices contain a user's "sensitive and confidential information,"[30] which is stored in a single, convenient location for examination.[31] The nature and quantity of information capable of being stored on an electronic device supports the proposition that law enforcement wishing to conduct a forensic search at the border should not be permitted to do so without some degree of particularized suspicion.[32] Either the Supreme Court or the legislature must speak on this issue in the near future to ensure that such invasive searches are only conducted when truly necessary in the interest of national security.[33]

This Note begins by exploring the current CBP policy surrounding the border search exception as it relates to electronic devices. Section II addresses the border search exception, the general requirements for

27. *Id.*

28. *Id.* at 1231.

29. *See Kolsuz*, 890 F.3d at 145 (recognizing that "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—and thus subjected to a routine border search—in luggage or a car.").

30. "[E]lectronic devices often retain sensitive and confidential information far beyond the perceived point of erasure, notably in the form of browsing histories and records of deleted files." United States v. Cotterman, 709 F.3d 952, 965 (9th Cir. 2013).

31. Laura K. Donohue, *Customs, Immigration, and Rights: Constitutional Limits on Electronic Border Searches*, 128 YALE L.J.F. 961, 965–966 (2019) (noting searches of modern cell phones reveal "[f]ar more information than law enforcement would be able to obtain by executing a physical warrant."). Donohue provides a helpful example by comparing the search of a home to the search of a cell phone. Where law enforcement obtains a warrant to search a home, the search is limited to what is described in the warrant. The search of a cell phone, however, reveals vastly more information about the individual, including personal contacts, photographs, videos, GPS records, and more. Donohue explains: "It is the equivalent of looking not just at an individual's home, but entering their bank, their car, and their workplace; accompanying them on dates and on social occasions; going to the PTA meeting with them, or to their local grocery store or mall; attending their places of worship; and sitting down next to them at the public library to make a record of everything they read." *Id.* at 965.

32. Rechtin, *supra* note 18, at 85–87 (arguing that despite the federal courts' articulated "suspicionless" standard for searches of electronic devices at the border, a "reasonable suspicion" standard should apply to these searches).

33. Will Carroll, *"Please Unlock Your Phone": Why Reasonable Suspicion Should be Extended to Cursory Searches of Electronic Devices at the Border*, 107 KY. L.J.O. 1, 13 (2018) (arguing that legislative action would be the most effective means to implement a requirement for reasonable suspicion for searches of electronic devices at the border, but that initiative by federal courts would directly influence changes in CBP's policies).

searches under the Fourth Amendment, the distinction between routine and nonroutine searches, and the unique circumstances created by the emergence of electronic devices such as laptops and smartphones in everyday life. Section III addresses the circuit split between the Fourth and Eleventh Circuits as to the standard to be applied when border agents wish to forensically search electronic devices at the border. Section IV advocates for a requirement of, at minimum, reasonable suspicion. Section V concludes.

II. FORENSIC SEARCHES OF ELECTRONIC DEVICES AT THE BORDER

The search of electronic devices at the border is undertaken by CBP, which has issued several directives addressing the ability of customs agents to search, copy, and share digital information stored in a traveler's electronic device.[34] The most recent CBP directive, issued in January 2018, defines "electronic device" as "any device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music, and other media players."[35] Searches of such devices are justified because they help federal agents to discover "evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography."[36]

According to the Department of Homeland Security (DHS), more than 397 million international travelers were processed by CBP officers during the 2017 fiscal year.[37] Of these incoming travelers, only 29,200 (approximately 0.007%) were subjected to a search of their electronic devices.[38] This is an increase from the 0.005% of international travelers subjected to searches of their electronic devices in 2016.[39] According to this data, few travelers are actually subjected to searches of their devices at the border. However, it is not the *number of actual searches* that should strike fear into any individual planning to travel internationally; it is the *practically unrestricted ability* of CBP to search every device that crosses the border. Thus, every traveler that crosses the border with an electronic

34. *See* U.S. CUSTOMS AND BORDER PROT., CBP DIRECTIVE NO. 3340-049A, BORDER SEARCH OF ELECTRONIC DEVICES (2018).

35. *Id.* at 2.

36. *Id.* at 1.

37. *CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics*, U.S. CUSTOMS AND BORDER PROT. (Jan. 5, 2018), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and [https://perma.cc/X4G9-NTFZ].

38. *Id.*

39. *Id.*

device (a smartphone, computer, tablet, etc.) is affected by the current policy.

While CBP has broad authority to conduct searches at the border in the interest of national security, as a policy matter, DHS has imposed certain requirements of their own "to ensure that the authority for border search of electronic devices is exercised judiciously, responsibly, and consistent with the public trust."[40] Pursuant to the most recent directive, a CBP officer may perform an "advanced" search of an electronic device where "there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern, and with supervisory approval at the Grade 14 level or higher."[41]

In earlier cases involving the search of electronic devices (primarily laptops) at the border, customs agents performed a manual search of the device, "clicking through the desktop, media folders, and internet history to identify evidence of illegal activity."[42] More recently, however, CBP agents have begun conducting forensic searches, which are by all measures significantly more intrusive with respect to the traveler's privacy.[43]

Forensically searching a traveler's electronic device involves more than merely thumbing through an individual's photos or contacts.[44] Computer forensics is a field encompassing the "methodologies used to collect, preserve, and examine" data from electronic storage devices.[45] A forensic search of an electronic device is generally conducted by an expert analyst who uses a range of software programs to comb through enormous

40. U.S. CUSTOMS AND BORDER PROT., CBP DIRECTIVE NO. 3340-049A, BORDER SEARCH OF ELECTRONIC DEVICES at 4 (2018).

41. *Id.* at 5.

42. *Id.*

43. *Id.* What CBP terms an "advanced search" involves a border agent connecting the device to "external equipment" to "review, copy and/or analyze its contents." This is much more invasive than the "basic search" which involves an agent examining the device itself and "information encountered at the border."

44. The January 2018 CBP Directive makes reference to both "basic" and "advanced" searches. "In the course of a basic search, with or without suspicion, an Officer may examine an electronic device and may review and analyze information encountered at the border, subject to the requirements and limitations provided herein and applicable law." An "advanced search" is defined by CBP as "any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents." U.S. CUSTOMS AND BORDER PROT., CBP DIRECTIVE NO. 3340-049A, BORDER SEARCH OF ELECTRONIC DEVICES at 4–5 (2018).

45. Wayne Jekot, *Computer Forensics, Search Strategies, and the Particularity Requirement*, 7 U. PITT. J. TECH. L. & POL'Y 2, 6 (2007).

amounts of data, which can take days, weeks, or even months.[46] Notably, this software is also capable of retrieving files that have been deleted, increasingly the amount of digital information available to the government during the search.[47]

III. THE FOURTH AMENDMENT AND THE BORDER SEARCH EXCEPTION

A. The Fourth Amendment's "Reasonableness" Requirement

The Fourth Amendment protects both searches and seizures.[48] "A 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed."[49] Whether an individual's constitutional rights have been violated thus depends on whether or not his privacy expectation is "one that society is prepared to recognize as reasonable."[50] A determination of whether a search is reasonable depends on the context in which the search occurred, and courts have frequently employed a balancing test, weighing "the need to search against the invasion which the search entails."[51]

Generally, the Fourth Amendment requires law enforcement to obtain a warrant, which requires a finding of probable cause, before conducting a search.[52] In determining what constitutes probable cause, the central question is whether the government official had a reasonable basis for believing the law was being violated; if the facts asserted are "such that a reasonably discreet and prudent man would be led to believe that there was a commission of the offense charged, there is probable cause justifying the issuance of a warrant."[53] Probable cause is not a technical standard; its definitions are based on "a reasonable ground for belief of guilt" that amounts to "more than bare suspicion."[54]

---

46. Orin S. Kerr, *Searches & Seizures in A Digital World*, 119 HARV. L. REV. 531, 537–38 (2005).

47. Sean O'Grady, Note, *All Watched Over by Machines of Loving Grace: Border Searches of Electronic Devices in the Digital Age*, 87 FORDHAM L. REV. 2255, 2270 (2019).

48. "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." U.S. CONST. amend. IV.

49. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

50. Carpenter v. United States, 138 S.Ct. 2206, 2213 (2018).

51. New Jersey v. T.L.O., 469 U.S. 325, 337 (1985) (quoting Camara v. Mun. Court, 387 U.S. 523, 537 (1967)).

52. Rankin, *supra* note 7, at 301.

53. Dumbra v. United States, 268 U.S. 435, 441 (1925).

54. Brinegar v. United States, 338 U.S. 160, 175–76 (1949) (quoting McCarthy v. De Armit, 99 Pa. 63, 69 (Pa. 1881)).

Even without probable cause, a law enforcement officer may lawfully execute a limited search and seizure where he "observes unusual conduct which leads him reasonably to conclude in light of his experience that criminal activity may be afoot."[55] The "reasonable suspicion" standard articulated in *Terry v. Ohio* requires that an officer be able to point to "specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion."[56] The officer's conduct is judged based on an objective standard—would a reasonable person in the officer's position agree that the action was appropriate?[57] "The Fourth Amendment does not require a policeman who lacks the precise level of information necessary for probable cause to arrest to simply shrug his shoulders and allow a crime to occur or a criminal to escape."[58]

B. The Border Search Exception

While searches generally require a warrant issued on a finding of probable cause, searches at the U.S. border are "reasonable" based solely on where they occur due to "the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country."[59] What is now known as the border search exception was first recognized by the Supreme Court as early as 1886[60] and is premised on protecting the integrity of our nation's border.[61] The doctrine serves the governmental interest of national security by preventing travelers from bringing potentially harmful things into the U.S., such as "communicable diseases, narcotics, or explosives."[62] When crossing the U.S. border, then, travelers are presumed to have a diminished expectation of privacy as compared to elsewhere.[63]

55. Terry v. Ohio, 392 U.S. 1, 30 (1968).

56. *Id.* at 21.

57. *Id.* at 21–22.

58. Adams v. Williams, 407 U.S. 143, 145 (1972).

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

60. Gregory T. Arnold, *Criminal Law—Bordering on Unreasonableness?: The Third Circuit Again Expands the Borders Search Exception in United States v. Hyde*, 40 VILL. L. REV. 835, 842 (1995) (noting that the first case to recognize the border search exception was Boyd v. United States, 116 U.S. 616 (1886)).

61. United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985).

62. *Id.* at 544.

63. "[A] port of entry is not a traveler's home. His right to be let alone neither prevents the search of his luggage nor the seizure of unprotected, but illegal, materials when his possession of them is discovered during such a search." United States v. Ramsey, 431 U.S. 606, 618 (citing United States v. Thirty-Seven Photographs, 402 U.S. 363, 376 (1971)).

The border search doctrine has been held to apply not only to searches conducted at the *actual* border but also to searches conducted at its "functional equivalent," such as an international airport.[64] It is also worth noting that the border search exception applies with equal force to travelers crossing the U.S. border for the purpose of entering the country as well as those exiting.[65]

C. Routine vs. Nonroutine Searches at the Border

Border searches may be characterized as "routine" or "nonroutine" based on the "degree and nature of the intrusiveness involved."[66] The Supreme Court has made it clear that routine searches at the border may be conducted without any degree of individualized suspicion.[67] More intrusive, nonroutine searches, however, may only be performed where law enforcement has reasonable suspicion.[68] Searches of a traveler's "outer clothing, luggage, and personal effects" have been classified as routine searches, while more physically intrusive searches like "strip searches, alimentary canal searches, x-rays, and the removal of an artificial limb" are nonroutine searches that require reasonable suspicion.[69]

D. Technology & the Border Search Exception

A series of cases have addressed the applicability of the border search exception to searches of electronic devices.[70] This body of case law suggests that courts must reconsider the border search exception where law enforcement conducts searches of electronic devices.[71]

64. Roberto Iraola, *Terrorism, the Border, and the Fourth Amendment*, FED. CTS. L. REV. 1, para. 19 (2003) (noting that "a search and seizure that does not technically occur at the border may still fall within the border search exception, as long as it takes place at the functional equivalent of the border.").

65. United States v. Oriakhi, 57 F.3d 1290, 1296–97 (4th Cir. 1995).

66. Iraola, *supra* note 64, at para. 12.

67. *Montoya de Hernandez*, 473 U.S. at 538.

68. *Id*. at 541 (holding "[t]he detention of a traveler at the border, beyond the scope of a routine customs search and inspection, is justified at its inception if customs agents, considering all the facts surrounding the traveler and her trip, reasonably suspect that the traveler is smuggling contraband in her alimentary canal.").

69. United States v. Kolsuz, 185 F. Supp. 3d 843, 853 (E.D. Va. 2016).

70. *See, e.g.*, United States v. Ickes, 393 F.3d 501 (4th Cir. 2005); United States v. Touset, 890 F.3d 1227 (11th Cir. 2018); United States v. Kolsuz, 890 F.3d 133 (4th Cir. 2018); United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013).

71. O'Grady, *supra* note 47, at 2280.

In *United States v. Ickes*, a traveler attempted to enter the U.S. from Canada when border agents searched his van, finding a computer and disks containing child pornography.[72] Ickes filed a motion to suppress the evidence from the computer and disks, arguing the search was unconstitutional.[73] The district court determined that the search did not require a warrant pursuant to the border search exception and denied Ickes's motion.[74] The Fourth Circuit affirmed[75]: "[S]ince the birth of our country, customs officials have wielded broad authority to search the belongings of would-be entrants without obtaining a warrant and without establishing probable cause."[76] The Fourth Circuit emphasized the strong governmental interest in preventing contraband (here, child pornography) from entering the country and the traveler's diminished expectation of privacy at the border.[77]

Three years later in *United States v. Arnold*, the Ninth Circuit considered whether federal agents at an international airport could lawfully search a traveler's computer without reasonable suspicion.[78] Arnold, returning to the United States from the Philippines, was stopped by CBP officers who searched his laptop and electronic storage devices, which contained child pornography.[79] Arnold was charged with transporting and possessing child pornography and attempting to engage in illicit sexual conduct.[80] Arnold moved to suppress the evidence obtained from his devices, which the district court granted after determining reasonable suspicion was required and that the government lacked reasonable suspicion at the time of the search.[81] On appeal, the Ninth Circuit reversed, holding that "reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border."[82]

The Ninth Circuit revisited border searches of electronic devices in *United States v. Cotterman* in 2013.[83] Cotterman attempted to enter the United States from Mexico when border agents confiscated his two

72. United States v. Ickes, 393 F.3d 501, 502–03 (4th Cir. 2005).
73. *Id.* at 503.
74. *Id.*
75. *Id.* at 507–08.
76. *Id.* at 505.
77. *Id.* at 506.
78. *See* United States v. Arnold, 533 F.3d 1003 (9th Cir. 2008).
79. *Id.* at 1005.
80. *Id.* at 1005–06.
81. *Id.*
82. *Id.* at 1008.
83. *See* United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013).

laptops and three digital cameras.[84] Cotterman was previously convicted of several sex-related offenses, producing a "hit" in the Treasury Enforcement Communication System.[85] Cotterman's devices were forensically searched.[86] An initial search of one of the laptops revealed hundreds of images of child pornography.[87] Cotterman was indicted for a plethora of child pornography offenses and moved to suppress the evidence obtained from his devices.[88] The district court granted Cotterman's motion after agreeing with the magistrate that the search was an "extended border search" requiring reasonable suspicion[89] and that the government lacked reasonable suspicion at the time of the search.[90]

In its analysis, the Ninth Circuit acknowledged the strong governmental interest in protecting our nation's borders but recognized the border search exception is a narrow one.[91] "Even at the border, individual privacy rights are not abandoned but 'balanced against the sovereign's interests.'"[92] While the initial search of Cotterman's devices was appropriate even without any degree of suspicion, the search was "transformed into something far different" when the devices were taken off the premises and forensically analyzed.[93] "It is the comprehensive and intrusive nature of a forensic examination—not the location of the examination—that is the key factor triggering the requirement of reasonable suspicion here."[94]

---

84. *Id.* at 957. The Treasury Enforcement Communications System (referred to as "TECS") is owned and managed by U.S. Customs and Border Protection. The system allows border agents to screen and make determinations regarding admissibility of travelers entering the U.S. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT UPDATE FOR THE TECS SYSTEM: CBP PRIMARY AND SECONDARY PROCESSING (TECS) NATIONAL SAR INITIATIVE (2011), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-tecs-sar-update_0.pdf [https://perma.cc/DV5A-M83S].

85. *Cotterman*, 709 F.3d at 957.

86. *Id.* at 958.

87. *Id.* at 959.

88. *Id.*

89. An extended border search is characterized as a "search away from the border where entry is not apparent, but where the dual requirements of reasonable certainty of a recent border crossing and reasonable suspicion of criminal activity are satisfied." *Id.* at 961 (citing United States v. Guzman-Padilla, 571 F.3d 865, 878–79 (9th Cir. 2009)). The extended border search is premised on the notion that once an individual crosses the border, he regains a substantial privacy interest. *Id.* at 961. Since the intrusion is greater, the government needs reasonable suspicion to justify an extended border search. *Id.* The Ninth Circuit ultimately found the extended border search doctrine inapplicable. *Id.* at 962.

90. *Id.* at 959.

91. *Id.* at 960.

92. *Id.* (citing United States v. Montoya de Hernandez, 473 U.S. 531, 539 (1985)).

93. *Id.* at 961.

94. *Id.* at 962.

In coming to the conclusion that forensic searches require reasonable suspicion, the Ninth Circuit pointed to the immense amount of data that modern electronic devices are capable of housing.[95] Digital storage devices have the potential to contain exponentially more information than "a car full of packed suitcases" ever could.[96] The court also noted the sensitivity and personal nature of the information typically stored on electronic devices: "Laptop computers, iPads and the like are simultaneously offices and personal diaries. They contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails."[97] Based on these considerations, the Ninth Circuit held that the forensic search of Cotterman's devices required a showing of reasonable suspicion by the government.[98]

In 2014, the Supreme Court had the opportunity in *Riley v. California* to consider whether law enforcement could search cell phones seized incident to the arrests[99] of defendants in two consolidated cases.[100] In the first case, police stopped Riley for driving with expired registration tags, and he was arrested after officers found two handguns in the vehicle.[101] Police confiscated and searched Riley's cell phone, revealing evidence of Riley's involvement in gang activity.[102] Riley sought to suppress the information obtained from his cell phone, asserting the search was unconstitutional because it was conducted without a warrant.[103] The trial court rejected Riley's argument, and the California Court of Appeals affirmed.

In the second case, police arrested Wurie after observing what they believed to be a drug deal. After taking him back to the station, officers confiscated Wurie's two cell phones and used information from one of the phones to locate Wurie's apartment.[104] Upon obtaining a warrant, officers found "crack cocaine, marijuana, drug paraphernalia, a firearm and

95. *Id.* at 964.
96. *Id.*
97. *Id.*
98. *Id.* at 968.
99. The "search incident to arrest" exception to the warrant requirement is different from the border search doctrine that has been discussed thus far. "Search of the person becomes lawful when grounds for arrest and accusation have been discovered, and the law is in the act of subjecting the body of the accused to its physical dominion." United States v. Robinson, 414 U.S. 218, 232 (1973) (quoting People v. Chiagles, 237 N.Y. 193, 197 (N.Y. 1923)).
100. Riley v. California, 573 U.S. 373 (2014).
101. *Id.* at 378.
102. *Id.* at 379.
103. *Id.*
104. *Id.* at 373.

ammunition, and cash."[105] Wurie sought to suppress the evidence from his apartment, asserting "it was the fruit of an unconstitutional search of his cell phone."[106] The district court disagreed with this argument, and Wurie was convicted. The First Circuit reversed, finding cell phones "distinct from other physical possessions that may be searched incident to arrest without a warrant."[107]

On appeal, the Supreme Court found that law enforcement generally must secure a warrant before searching a cellular device even where the search is pursuant to an arrest, recognizing the unique nature of cell phones and the digital content they store.[108] The *Riley* Court called the term "cell phone" a "misleading shorthand" because of its immense storage capacity and the sensitive nature of the personal data such devices are capable of storing.[109] To make matters worse, cloud computing increases the amount of data accessible from the search of an electronic device, as data may be "stored on remote servers rather than on the device itself."[110]

In *United States v. Vergara* in 2018, the Eleventh Circuit found the forensic search of a traveler's cell phones at the border to be lawful even without a warrant or probable cause. When Vergara returned from a trip to Mexico, CBP officers stopped him and searched one of his phones. The officers discovered a video of partially nude minors, submitted all of Vergara's phones for forensic analysis, and discovered more photos and videos depicting sexually explicit conduct involving minors. Vergara sought to suppress this evidence, but the district court found the search was lawful and did not require any degree of particularized suspicion. In doing so, the court rejected Vergara's argument that the Supreme Court's decision in *Riley* required a warrant for the forensic search, finding *Riley*'s holding limited to the search incident to arrest exception and having no application to border searches. The district court reasoned that regardless of whether any degree of suspicion was required, the officers in this case had reasonable suspicion that Vergara possessed child pornography. The Eleventh Circuit affirmed.[111]

105. *Id.* at 381.
106. *Id.*
107. *Id.*
108. *Id.* at 386.
109. *Id.* at 393.
110. *Id.* at 397.
111. United States v. Vergara, 884 F.3d 1309, 1311–13 (11th Cir. 2018).

IV. KOLSUZ & TOUSET: DIFFERING OPINIONS BETWEEN THE FOURTH AND ELEVENTH CIRCUITS

A. United States v. Kolsuz (Fourth Circuit)

Hamza Kolsuz, a Turkish citizen, attempted to board an international flight when he was stopped by federal customs agents. On two prior occasions, Kolsuz attempted to transport firearms parts listed on the United States Munitions List ("USML")[112] into the U.S. without an appropriate license. Upon learning that Kolsuz would be travelling back to Turkey, a border agent alerted CBP officers at the airport. A search of Kolsuz's luggage revealed several firearm parts listed on the USML, which Kolsuz lacked the requisite federal license to remove from the country.[113]

The customs officers conducted two searches of Kolsuz's smartphone: first, a manual search, then a forensic search. The manual search "involved using the iPhone's touch screen, which was not password protected, to scroll through Kolsuz's recent calls and text messages." The cell phone was taken four miles away from the airport and connected to a "Cellebrite Physical Analyzer," which produced an 896-page report detailing Kolsuz's "personal contact lists, emails, messenger conversations, photographs, videos, calendar, web browsing history, and call logs, along with a history of Kolsuz's physical location down to precise GPS coordinates."[114]

Kolsuz was indicted on counts of "attempting to export firearms parts on the USML without a license . . . attempting to smuggle goods from the United States . . . and conspiracy to commit those offenses."[115] Kolsuz sought to suppress the evidence obtained from the forensic search, arguing the search was "nonroutine" and required reasonable suspicion.[116] The district court denied Kolsuz's motion.[117] While the district court found the forensic search to be "nonroutine," and thus required some degree of particularized suspicion,[118] the search was reasonable because the government had reasonable suspicion Kolsuz's phone would provide

112. The United States Munitions List (USML) is comprised of "defense articles and defense services" whose importation and exportation are regulated by the federal government through the Arms Export Control Act. *See* 22 U.S.C.A. § 2778 (2014).

113. United States v. Kolsuz, 890 F.3d 133, 138–139 (4th Cir. 2018).

114. *Id.* at 139.

115. *Id.*

116. *Id.*

117. United States v. Kolsuz, 185 F. Supp. 3d 843, 860 (E.D. Va. 2016).

118. *Id.* at 858.

evidence relevant to the charged crimes.[119] Kolsuz was found guilty on all counts and "sentenced to 30 months in prison and three years of supervised release."[120]

Kolsuz's appeal to the Fourth Circuit was narrowly focused on whether the second search of his cell phone—the forensic search—fell within the border search exception. Kolsuz first argued the forensic search was too far removed in time and space from Kolsuz's departure to be considered a border search and should be treated as a search incident to arrest, requiring a warrant based on probable cause. In arguing the forensic search was not a border search, Kolsuz emphasized that "the government interest that underlies the border search exception—preventing contraband from crossing a border—was no longer at issue" because Kolsuz was arrested, and his phone had already been confiscated at the time of the search.[121]

The Fourth Circuit rejected Kolsuz's arguments, finding a sufficient "nexus" between the forensic search and the government's interest in performing the search. In finding such a connection, the court analyzed the factual circumstances surrounding the search:

> Government agents forensically searched Kolsuz's phone because they had reason to believe—and good reason to believe, in the form of two suitcases filled with firearms parts—that Kolsuz was attempting to export firearms illegally and without a license. That is a transnational offense that goes to the heart of the border search exception, which rests in part on the sovereign interest of protecting and monitoring exports from the country.[122]

The Fourth Circuit concluded that the forensic search of Kolsuz's phone fell squarely within the border search exception.[123] Even so, Kolsuz argued, the forensic search was nonroutine and thus "require[ed] some level of particularized suspicion"—an argument well taken by the court.[124] Recognizing that even border searches may require some degree of suspicion if sufficiently intrusive, the Fourth Circuit noted that "the sheer quantity of data stored on smartphones and other digital devices

119. *Id.* at 860.

120. *Kolsuz*, 890 F.3d at 139–41.

121. *Id.* at 141–42. Kolsuz argued that the forensic search, which took place "miles from the airport," was no longer a border search at all. Kolsuz argued that the search, although conducted after Kolsuz's arrest, required a warrant pursuant to the Supreme Court's holding in *Riley* that cell phones may only be searched incident to a lawful arrest upon a finding of probable cause and issuance of a warrant. *Id.* (citing Riley v. California, 573 U.S. 373, 401–02 (2014)).

122. *Kolsuz*, 890 F.3d at 143.

123. *Id.* at 144.

124. *Id.*

dwarfs the amount of personal information that can be carried over a border—and thus subjected to a routine border search—in luggage or a car."[125]

The Fourth Circuit proceeded to address the "uniquely sensitive nature" of the information obtained from forensic searches of electronic devices, which often includes "financial records, confidential business documents, medical records, and private emails."[126] The court characterized this data as being comprised of "the most intimate details of our lives" and recognized that international travelers cannot simply leave this electronic information at home in the same way they could leave behind other tangible items that they do not wish to subject to a search.[127]

The Fourth Circuit concluded that "[a] forensic search of a digital phone must be treated as a nonroutine border search, requiring some form of individualized suspicion."[128] Since the customs officers had reasonable suspicion to conduct the forensic search of Kolsuz's phone, the Fourth Circuit affirmed the district court's decision.[129]

B. United States v. Touset (Eleventh Circuit)

After investigations revealed multiple monetary transfers to an account in the Philippines— a "source countr[y] for sex tourism and child pornography"—the U.S. government suspected Touset was involved in child pornography. Since Touset was out of the country at the time, DHS "placed a 'look-out' on Touset so that his luggage and electronic devices would be searched when he returned to the country."[130]

Upon returning to the U.S., a border agent searched his luggage, finding "two iPhones, a camera, two laptops, two external hard drives, and two tablets." The agent manually inspected the phones and camera, and the laptops, hard drives, and tablets were subjected to a forensic search, revealing child pornography. Touset was indicted on counts of "knowingly receiving child pornography, . . . knowingly transporting and shipping child pornography, . . . and knowingly possessing a computer and storage device containing child pornography."[131]

Touset sought to suppress the evidence obtained from the forensic searches. The magistrate determined the search required reasonable

125. *Id.* at 145.
126. *Id.*
127. *Id.* at 145.
128. *Id.* at 145–47.
129. *Id.* at 146–48.
130. United States v. Touset, 890 F.3d 1227, 1230 (11th Cir. 2018).
131. *Id.* at 1230–31.

suspicion, and that the government had reasonable suspicion at the time of the search. The district court adopted the magistrate's recommendation that Touset's motion to suppress be denied. Touset pleaded guilty to knowingly transporting child pornography and was sentenced to "120 months in prison and supervision for life."[132]

The Eleventh Circuit reaffirmed the proposition that routine searches conducted at the border are reasonable simply on the basis that they occur at the border. Moreover, the court noted that neither the Eleventh Circuit nor the Supreme Court has ever required any degree of suspicion to search travelers' property at the border regardless of the "type" of property that was the subject of the search. Based on this unforgiving precedent, the court "[saw] no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property."[133]

Reasonable suspicion has been required, the Eleventh Circuit acknowledged, for "highly intrusive searches of a person's body" at the border such as strip searches or x-ray examinations, which are notably different than any search of a person's belongings. The court cited three factors which may be used to identify the "indignity" to be suffered by an individual subjected to a nonroutine search: "(1) physical contact between the searcher and the person searched; (2) exposure of intimate body parts; and (3) use of force." The Eleventh Circuit found none of these factors applicable to a forensic search.[134]

The Eleventh Circuit compared the forensic search of Touset's devices to the physical search of a vehicle's fuel tank seen in *Flores-Montano.*[135] The court reasoned:

> And it does not make sense to say that electronic devices should receive special treatment because so many people now own them or because they can store vast quantities of records or effects. The same could be said for a recreational vehicle filled with personal effects or a tractor-trailer loaded with boxes of documents. Border agents bear the same responsibility for preventing the importation of contraband in a traveler's possession regardless of advances in technology.[136]

The Eleventh Circuit acknowledged, but ultimately rejected, the differing opinions of the Fourth Circuit in *Kolsuz* and the Ninth Circuit in

132. *Id.* at 1231.
133. *Id.* at 1232–33.
134. *Id.* at 1234.
135. *See* United States v. Flores-Montano, 541 U.S. 149 (2004).
136. *Touset*, 890 F.3d at 1233.

Cotterman. The court noted that it is not the "extensiveness" of a search that matters but the "personal indignity" suffered. The court emphasized that "property and persons are different," and the search of digital data does not "trigger this kind of indignity."[137]

The Eleventh Circuit, balancing the two interests at stake, concluded that the government's interest in excluding certain persons and contraband from the border outweighs a traveler's privacy interest. When crossing the border, the court reasoned, an individual's expectation of privacy is diminished and there is no constitutional "guarantee [to] the right to travel without great inconvenience." To the contrary, travelers should expect some degree of inconvenience as incident to achieving a greater common good—national security. If a traveler does not want to subject his personal property to a search, the court reasoned, he can eliminate that risk by leaving his devices at home.[138]

If reasonable suspicion was required to conduct the forensic search of Touset's devices, the Eleventh Circuit believed it would "create special protection for the property most often used to store and disseminate child pornography."[139] Offenses relating to child pornography heavily utilize the internet and electronic devices for the "receipt, storage and distribution of unlawful images."[140] The court reasoned that requiring reasonable suspicion to conduct forensic searches would impede the government's interest in excluding this type of contraband from our nation's borders.[141] In fact, the Eleventh Circuit went even further, suggesting the overwhelming presence of technology in our society actually weighs *in favor* of the government's broad discretion to search travelers' devices at the border.[142]

Rather than imposing a reasonable suspicion requirement through the judiciary, the Eleventh Circuit recommended leaving the task of setting the appropriate standard to the legislative process, as this would allow for a more informed decision on the matter. The court suggested that deferring to the legislature in the area of border searches is "especially important," and there has been a "longstanding historical practice" of doing so.[143]

137. *Id.* at 1234.
138. *Id.* at 1235.
139. *Id.*
140. *Id.* at 1236.
141. *Id.* at 1235–36.
142. *Id.* at 1235.
143. *Id.* at 1236–37.

As in *Kolsuz*, a determination of whether any degree of suspicion is required to conduct a forensic search at the border was not outcome-determinative in *Touset* because the Eleventh Circuit found the government had a "particularized and objective basis" to search Touset's devices for child pornography.[144]

V. A CALL FOR CHANGE: THE CURRENT "SUSPICIONLESS STANDARD" AND THE NEED FOR INDIVIDUALIZED SUSPICION

A. Tension Between Circuits and the Need for Consistency

The Fourth and Eleventh Circuit's differing conclusions emphasize a gray area in the border search exception as travelers cross the border with electronic devices not likely conceived of when the doctrine was established.[145] The Fourth Circuit in *Kolsuz* recognized the unique challenges of our digital world—forensic searches of electronic devices may be especially intrusive with respect to a traveler's privacy interest and thus should be treated differently than manual searches.[146] The Eleventh Circuit in *Touset*, on the other hand, refused to make a distinction between classes of property searched at the border.[147]

Following *Kolsuz* and *Touset*, the Seventh Circuit in *United States v. Wanjiku* found the search of a traveler's electronic devices at the border constitutional because agents acted on reasonable suspicion "at a time when no court had ever required more than reasonable suspicion for any search at the border."[148] Interestingly, the defendant in *Wanjiku* argued that searches of electronic devices are nonroutine, requiring at least reasonable suspicion and arguably even a *warrant*.[149] Because the officers had reasonable suspicion, the Seventh Circuit declined to identify any particular standard as the appropriate level of scrutiny for border searches of electronic devices: "We therefore need not reach the issue of what level of suspicion is required (if any) for searches of electronic devices at the border, and reserve that question for a case in which it matters to the outcome."[150]

144. *Id.* at 1237.

145. *See, e.g.*, United States v. Kolsuz, 890 F.3d 133 (4th Cir. 2018); United States v. Touset, 890 F.3d 1227 (11th Cir. 2018).

146. *Kolsuz*, 890 F.3d at 144–46.

147. *Touset*, 890 F.3d at 1233.

148. United States v. Wanjiku, 919 F.3d 472, 479 (7th Cir. 2019).

149. *Id.* at 478.

150. *Id.* at 488–89.

Wanjiku demonstrates the uncertainty courts face in the wake of *Kolsuz* and *Touset* and the dissonance among circuits. The question remains: at the border, should electronic devices be subject to the same standard as routine searches, or do these devices present unique privacy considerations that warrant application of higher scrutiny? While there are differing opinions surrounding what the appropriate standard may be,[151] consistency is needed to serve both the governmental interest in national security and the privacy interests of international travelers.[152]

B. Electronic Devices Are More than Mere "Containers"

It has been argued that the "suspicionless" standard is most appropriate because it "avoids the creation of arbitrary distinctions between different types of property" and more effectively deters criminal activity.[153] Some commentators have even asserted that treating electronic devices in the same manner as "traditional" storage devices is logical because they serve the same functional purpose: storage.[154] But the ability of electronic devices to store a large quantity of "deeply personal" or "embarrassing" information about the device's user requires a distinction between searches of electronic devices from searches of other personal items belonging to a traveler, such as "wallets, purses, luggage, and other containers."[155]

Contrary to the Eleventh Circuit's view in *Touset*, an electronic device is starkly different than a "tractor-trailer loaded with boxes of

151. Aisha J. Dennis, *Riling Up the Border Search Doctrine: Litigating Searches of Digital Content at Our Ports of Entry*, THE CHAMPION, March 2018 at 40, 44 (arguing the appropriate level of suspicion required for federal officers to search electronic devices at the border is "currently an open question in light of *Riley v. California*," and that advocates should continue to update courts on technological advancements that make these searches different from traditional items of personal property normally subject to search).

152. With conflicting standards from CBP, the Fourth and Eleventh Circuits, and proposed legislation, there is uncertainty at the border for both travelers and law enforcement. Gina R. Bohannon, Notes & Comment, *Cell Phones and the Border Search Exception: Circuit Split Over the Line Between Sovereignty and Privacy*, 78 MD. L. REV. 563, 587 (2019).

153. Michael Creta, *A Step in the Wrong Direction: The Ninth Circuit Requires Reasonable Suspicion for Forensic Searches of Electronic Storage Devices During Border Searches in United States v. Cotterman*, 55 B.C.L. Rev. E-Supplement 31, 40–41 (2014) (arguing also that the focus should be on changing CBP directives to place stricter limits on the manner in which customs officers may store and retain information obtained from a forensic search of an electronic device at the border).

154. *Id.* at 41 ("Focusing on how information is used, as opposed to when it can be collected, is an administratively practical standard that avoids tampering with constitutional doctrine and also strikes an appropriate balance between border protection goals and personal privacy interests.").

155. Bret E. Rasner, *International Travelers Beware: No Reasonable Suspicion Needed to Search Your Electronic Storage Devices at the Border*, 3 PHOENIX L. REV. 669, 697 (2010).

documents."[156] The Fourth Circuit in *Ickes* addressed the issue of whether an electronic device is merely "cargo" or something more, ultimately finding the search of a traveler's computer and disks lawful pursuant to 19 U.S.C. § 1581(a), which authorizes customs officers to search "any person, trunk, package, or cargo on board [a vessel]."[157] In coming to this conclusion, the Fourth Circuit consulted Black's Law Dictionary, which defined "cargo" as "goods transported by a vessel, airplane, or vehicle."[158] The court determined that the computer and disks fell within the definition of "cargo," and "to hold otherwise would undermine the longstanding practice of seizing goods at the border even when the type of good is not specified in the statute."[159] Moreover, in light of the government's historical "power and interest" at the border, and courts' historically broad interpretation of § 1581(a), the Fourth Circuit found the search lawful.[160]

In his defense, Ickes asserted that the court's holding was sweeping because "any person carrying a laptop computer . . . on an international flight would be subject to a search of the files on the computer hard drive."[161] The court characterized Ickes's prediction as "far-fetched" because agents at the border lack the time and resources to perform a search of every computer.[162] But the mere unlikeliness of such a search should not negate the constitutional implications it may have on those few individuals who are, in fact, subjected to a forensic search of their electronic devices at the border. In accordance with the current view that no suspicion is required to perform forensic searches at the border, any international traveler must assume the risk of their device being confiscated, forensically searched, and the data copied and stored.[163]

Electronic devices should not be thought of as closed containers due to the vast amount of information these devices are capable of storing as well as the uniquely private and sensitive nature of that information. Some have argued that, because of the quantity and sensitive quality of information produced, the search of an electronic device is akin to the

156. United States v. Touset, 890 F.3d 1227, 1233 (11th Cir. 2018).
157. United States v. Ickes, 393 F.3d 501, 505 (4th Cir. 2005).
158. *Id.* at 504 (citing BLACK'S LAW DICTIONARY (8th ed. 2004)).
159. *Ickes*, 393 F.3d at 505.
160. *Id.*
161. *Id.* at 506–07.
162. *Id.*
163. Rankin, *supra* note 7, at 319 ("In short, current federal policy permits the government to seize the computer of any person crossing the national border, make a complete copy of the hard drive, and then search through every file and folder until it discovers something illegal, all without any suspicion of criminal activity.").

search of a traveler's home.[164] Unlike a suitcase, a traveler's electronic device may contain "precious memories, important files, and confidential information all in one place" and often contains even more information about the traveler than her home would.[165] The average traveler likely expects to undergo routine searches in the interest of national security; at the airport, for example, travelers expect TSA agents to search their luggage for weapons that could injure others on the plane. But a traveler hardly expects their phone to be confiscated and digital data extracted.[166]

A key distinction between electronic devices and traditional "containers" lies in the fact that a forensic search of an electronic device will reveal not only data currently stored on the device but also information that has been deleted.[167] While a traveler can remove anything from his suitcase that he does not want to be searched, nothing can truly be removed from an electronic device.[168] Moreover, routine searches aimed primarily at promoting the government's interest in national security divulge little personal information about the traveler, whereas forensic searches of electronic devices "may reveal a person's entire life or career."[169] As technology improves, so does the quantity and diversity of the information capable of being stored on our digital devices, and eventually, forensic analysts may be capable of completely

164. The search of electronic devices differs from the search a traveler's wallet or briefcase because an electronic device "contains exponentially more information than wallets or briefcases and often contains information the owner does not know is stored on the device." Carolyn James, *Balancing Interests at the Border: Protecting Our Nation and our Privacy in Border Searches of Electronic Devices*, 27 SANTA CLARA HIGH TECH. L.J., 219, 222 (2011). Because a laptop search can often reveal as much information about a person as a search of that person's house would, traveling internationally with an electronic device is like "crossing the border with your home in your suitcase." *Id.* (quoting Ellen Nakashima, *Clarity Sought on Electronics Searches*, WASH. POST (Feb. 7, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/02/06/AR2008020604763.html [https://perma.cc/GEC8-TXRM & https://perma.cc/7SFL-SDZM].

165. Kindal Wright, *Border Searches in A Modern World: Are Laptops Merely Closed Containers, or Are They Something More?*, 74 J. AIR L. & COM. 701, 721–22 (2009).

166. Joelle Hoffman, *Reasonable Suspicion Should Be Required at A Minimum for Customs Officials to Execute A Search of A Laptop at U.S. Borders: Why* U.S. v. Arnold *Got It Wrong*, 36 W. ST. U. L. REV. 173, 181–82 (2009).

167. Kerr, *supra* note 46, at 542 ("[F]orensic analysts can often recover deleted files from a hard drive. They can do that because marking a file as "deleted" normally does not actually delete the fileFalse").

168. Robert M. Yost, *Deleting Privacy Bit by Bit: An Analysis of* U.S. v. Arnold *& Suspicionless Border Searches of Laptop Computers & Electronic Devices*, 19 TEMP. POL. & CIV. RTS. L. REV. 303, 318 (2009) (noting that electronic devices pose the unique problem of "lingering and pervasive data storage, whereby physical removal of its contents by its owner does not actually result in removal.").

169. Hoffman, *supra* note 166, at 182.

reconstructing a person's life "with remarkable accuracy" using the data stored on that individual's devices.[170]

In *Cotterman*, the Ninth Circuit distinguished electronic devices from other "containers," reasoning that a traveler can choose what he packs in his suitcase but cannot do the same with his electronic devices because deleting files may be impractical, time consuming, and deleted files may remain on the device nonetheless.[171] "This quality makes it impractical, if not impossible, for individuals to make meaningful decisions regarding what digital content to expose to the scrutiny that accompanies international travel. A person's digital life ought not be hijacked simply by crossing a border."[172]

In *Vergara*, the district court reasoned that if the defendant "entered the country with child pornography images in a notebook, the notebook would have been subject to inspection, and he cannot be allowed to insulate himself from inspection by storing child pornography electronically on his cellphone."[173] Surely, however, it cannot be contended that a notebook can hold the same amount of information capable of being stored on an electronic device.

Circuit Judge Jill Pryor's dissent in *Vergara* is insightful in considering how electronic devices differ from other "containers." Judge Pryor disagreed with "the majority's dismissal of the significant privacy interests implicated in cell phone searches" and recommended that forensic searches require "a warrant supported by probable cause." Our devices can expose sensitive personal information relating to "addiction, religious practices, pregnancy, personal finances, and romance."[174] It is unlikely the same can be said of a traveler's other belongings.

C. Forensic Searches Should be Considered "Nonroutine"

Perhaps the most important question that must be addressed in determining the appropriate standard for forensic searches of electronic devices at the border is one of scope: are nonroutine searches, for which reasonable suspicion is required, limited to searches of a traveler's person?[175] The Supreme Court should answer this question in the

170. Kerr, *supra* note 46, at 569.

171. United States v. Cotterman, 709 F.3d 952, 965 (9th Cir. 2013).

172. *Id.*

173. United States v. Vergara, 884 F.3d 1309, 1311 (11th Cir. 2018).

174. *Id.* at 1315–16 (Pryor, C.J., dissenting).

175. Lindsay E. Harrell, *Down to the Last .jpeg: Addressing the Constitutionality of Suspicionless Border Searches of Computers & One Court's Pioneering Approach in* United States v. Arnold, 37 SW. U. L. REV. 205, 222 (2008).

negative, extending the reasonable suspicion requirement to the forensic search of electronic devices.

Rather than viewing forensic searches as an extension of a manual search, such searches should be subject to the same standard as other highly intrusive or "particularly offensive" searches.[176] The rationale of the border search exception is based on national security and the ability of the federal government to interrupt the transportation of dangerous items such as "bombs, weapons, communicable diseases, narcotics, or explosives" across the U.S. border.[177] These kinds of "contraband" can be directly related to the immediate safety of American citizens, and one can understand why the federal government would want great discretion in searching for these items.[178] Forensic searches of electronic devices, however, do not comport with this "logical purpose" of the border search doctrine, nor do they comport with the public's understanding of border searches.[179] Further, while the Supreme Court has characterized the government's interest as "at its zenith" at the border, the *Riley* decision suggests that a traveler's privacy rights should be given additional protection when border agents wish to search her electronic device.[180]

For purposes of determining the appropriate standard, our electronic devices more closely resemble an extension of our person than tangible personal property.[181] Nonroutine searches have thus far been limited to searches of a traveler's person, as the Supreme Court has yet to find a search of traveler's property nonroutine.[182] However, because a forensic search of a traveler's device reveals so much detailed information about that individual, these searches should be characterized as nonroutine. In *Flores-Montano*, the Supreme Court recognized "the dignity and privacy interests of the person being searched" may require "some level of suspicion in the case of highly intrusive searches of the person."[183] Even

176. *See* United States v. Flores-Montano, 541 U.S. 149, 152 (2004); United States v. Montoya de Hernandez, 473 U.S. 531, 541–42 (1985) (Brennan, J., dissenting).

177. Victoria Wilson, *Laptops and the Border Search Exception to the Fourth Amendment: Protecting the United States Borders from Bombs, Drugs, and the Pictures From Your Vacation*, 65 U. MIAMI L. REV. 999, 1009 (2011).

178. *See* Wright, *supra* note 165, at 723 ("The purpose behind the broad scope of the border search exception to the Fourth Amendment is that the government is seeking to prevent the entry of contraband into the United States in order to protect its citizens.").

179. Wilson, *supra* note 177, at 1008–10.

180. Dennis, *supra* note 151, at 44.

181. Wright, *supra* note 165, at 722 ("[I]f the courts are looking to analogize laptops to something, they should find that computers are more accurately analogized to the human body than to a closed container.").

182. O'Grady, *supra* note 47, at 2257.

183. United States v. Flores-Montano, 541 U.S. 149, 152 (2004).

at the border, however, a traveler will be entitled to greater Fourth Amendment protection where the government seeks to employ "highly intrusive techniques."[184] One can imagine how forensic searches may fit into this category.

Courts have drawn what some commentators have identified as a "bright-line rule" between the intrusive search of a traveler's person and the search of a traveler's personal effects, suggesting the heightened privacy concerns of the traveler could not be asserted if it is merely his property that is subjected to search.[185] However, the Supreme Court has not foreclosed the idea that some searches of a traveler's property, although occurring at the border, may be "so intrusive that they require reasonable suspicion."[186]

While the forensic search of an electronic device is not *literally* intrusive into the traveler's person, as a strip search would be, it can be viewed as substantially intrusive into the traveler's mind.[187] The district court in *Arnold* noted that "some may value the sanctity of private thoughts memorialized on a data storage device above physical privacy."[188] It is certainly possible to imagine how a traveler would be willing to undergo a pat-down search of his person to detect a weapon or other dangerous object, as this seems perfectly logical with respect to the government's interest in national security. But forcing a traveler to subject her devices to a forensic search may constitute a "government intrusion[]into the mind"[189] that may cause any traveler to become

184. Bohannon, *supra* note 152, at 573.

185. Nicole Kolinski, United States v. Arnold*: Legally Correct but Logistically Impractical*, 6 J.L. ECON. & POL'Y 31, 44 (2009).

186. Marianne Leach, *Flyers Beware: The Ninth Circuit Decision, United States v. Arnold, Granted Customs Agents Access into Your Laptops*, 26 T.M. COOLEY L. REV. 307, 311 (2009), citing United States v. Flores-Montano, 541 U.S. 149, 154 n.2 (2004). *See also* United States v. Ramsey, 431 U.S. 606, 616 n.13 (1977) (declining to "decide whether, and under what circumstances, a border search might be deemed 'unreasonable' because of the particularly offensive manner in which it is carried out.").

187. United States v. Arnold, 454 F. Supp. 2d 999, 1003 (C.D. Cal. 2006).

188. *Id.* (recognizing that searching the digital contents of a laptop involves "dignity and privacy interests" in the same way that "highly intrusive searches of persons" do and the fact that it is not a "physical intrusion" does not place it outside the scope of Fourth Amendment protection).

189. Just as an individual's physical possessions can be intruded upon, the Ninth Circuit has suggested that there may be a "psychological intrusion" where an individual fears a particular search. "Imposition of fear is a psychological intrusion." United States v. Molina-Tarazon, 279 F.3d 709, 716 (9th Cir. 2002). *Flores-Montano* subsequently found the search at issue in *Molina-Tarazon* did not require reasonable suspicion; since the "thing" searched was a vehicle, which was not sufficiently intrusive, the Ninth Circuit's "complex balancing tests" were inappropriate. *Flores-Montano*, 541 U.S. at 152. However, the *Molina-Tarazon* decision is useful in identifying the right of citizens to be free not only from physical intrusions, but searches that are intrusive into one's mind. In evaluating the intrusiveness of electronic searches, psychological intrusiveness should be considered as a factor.

afraid.[190] In evaluating the intrusiveness of a forensic search, the Supreme Court should give considerable weight to the "psychological intrusion"[191] these types of searches are likely to affect. By recognizing forensic searches as "nonroutine" and requiring reasonable suspicion as a prerequisite for conducting these searches, the "unique privacy interests in digital data highlighted in *Riley* and *Carpenter*" could be acknowledged while upholding "the government's traditional right to secure and protect the border."[192]

D. Public Policy and Racial Profiling at the Border

Many international travelers of certain racial, ethnic, or religious groups already face increased scrutiny when traveling, and granting such broad discretion to border agents to conduct forensic searches of electronic devices makes privacy violations far more likely for these individuals.[193] While the issue of religious and racial profiling arises in many aspects of our society, it has significant consequence in the context of border searches. The government should retain the ability to search any individual's electronic devices where that individual is suspected of criminal activity, regardless of race or religion. But members of specific racial or religious groups should not be asked to expose sensitive personal information contained on their electronic devices solely on the basis of a border agent's personal biases.

As of August 10, 2017, DHS maintains that "[i]t is the policy of U.S. Customs and Border Protection (CBP) to prohibit the consideration of race or ethnicity in law enforcement, investigation, and screening activities, in all but the most exceptional circumstances" so that "racial and ethnic stereotypes will not be used in conducting stops, searches, and

190. Harrell, *supra* note 175, at 224–25 ("[A]n intrusion into a person's most private thoughts and expressions memorialized in electronic files could frighten or annoy a traveler passing through customs.").

191. *Molina-Tarazon*, 279 F.3d at 716.

192. O'Grady, *supra* note 47, at 2282. In *Carpenter*, the Supreme Court found that cell phone location data is within the protection of the Fourth Amendment even though the information was obtained from a third party. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018). While not discussed at length in this article, the *Carpenter* decision provides insight into the Supreme Court's view of technology in the Fourth Amendment context: "As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Id.* at 2214.

193. Jillian A. Bates, *The Forensic Digital Search of Cell Phones at the Border in* United States v. Kolsuz: *Tough on Terrorism or Tough on Petty Crime?*, 41 N.C. CENT. L. REV. 39, 43 (2019).

other law enforcement activities."[194] Just a few sentences later, the DHS policy states that "CBP personnel may use race or ethnicity when a compelling governmental interest is present and its use is narrowly tailored to that interest" and allows CBP officers to consider nationality "for the vast majority of situations" border agents may find themselves in.[195] The federal government seems to be condemning racial and ethnic profiling except where it serves a governmental interest, and as a result, border agents have a dangerous amount of discretion in determining which travelers to subject to extensive search.[196] Allowing border agents to conduct forensic searches subjectively, without imposing any objective standards, arguably undermines the ability of those agents to protect our borders.[197]

E. Making a Distinction Between Types of Contraband

Unlike other border searches, the governmental interest in national security does not justify warrantless searches of electronic devices at the border.[198] Most of the cases involving forensic searches of electronics at the border have involved child pornography,[199] while the types of contraband contemplated when the border search doctrine was first recognized are related to national security threats.[200] Certainly, it need not

194. *CBP Policy on Nondiscrimination in Law Enforcement Activities and all other Administered Programs*, U.S. CUSTOMS AND BORDER PROT., (August 10, 2017), https://www.cbp.gov/about/eeo-diversity/policies/nondiscrimination-law-enforcement-activities-and-all-other-administered# [https://perma.cc/3KVW-A94X].

195. *Id.* ("Race or ethnicity-based information that is specific to particular suspects or incidents or ongoing criminal activities, schemes, or enterprises may be considered.").

196. *See* Bector, *supra* note 13, at 711 (recognizing that a suspicionless standard "may lead to searches that are arbitrary, unnecessary, or involve racial profiling.").

197. Any traveler crossing the border—even those who pose no threat to national security—can be subjected to forensic search under the current standard, and "[c]onducting searches of persons on a subjective basis removes the ability of officers to conduct searches with the objective interest of protecting national security." Darianne De Leon, Comment, *What Matters More: Preserving a Fundamental Right to Privacy or Tampering with Another's Dignity Through Searches Because of "Reasonable Suspicion"*, 27 AM. U.J. GENDER SOC. POL'Y & L. 553, 567 (2019).

198. Wright, *supra* note 165, at 723–24 (arguing that a traveler who wants to get digital contraband into the United States need not physically cross a border to do so, as they can transmit the same information through email or by posting it to the internet).

199. Shannon L. Smith, *Abidor & House: Lost Opportunities to Sync the Border Search Doctrine with Today's Technology*, 40 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 223, 228 (2014).

200. While the original justifications for the border search exception were financial (based on collection of taxes), the Supreme Court later concluded that "national self protection" was an appropriate justification for allowing searches to occur at the border without a warrant. During the war on drugs, the doctrine was used to prevent the smuggling of narcotics across the United States border. Today, the doctrine has been extended to apply to the movement of any "dangerous items" across the border. Wilson, *supra* note 177, at 1003–1005.

be explained why the U.S. would seek to exclude child pornography from its borders; however, this type of contraband does not pose the same immediate threat to national security as a weapon or explosive.

Further, the border search exception should not be used as "general crime prevention"[201] as this creates potential for abuse and intrudes significantly "into the privacy of ordinary U.S. citizens."[202] In advocating for a requirement of some degree of particularized suspicion where border agents seek to forensically search a traveler's device, the goal is certainly not to encourage importation of contraband. However, the current policy is overinclusive, affecting millions of international travelers.[203] Moreover, unlike the "dangerous" forms of contraband that the border search exception historically sought to exclude from the country, the government's interest in excluding digital contraband is not any greater at the border.[204]

While a traveler would expect federal agents at the border to inspect his or her laptop's "*physical* inner workings" to make sure it does not contain an explosive, it is a different matter entirely to search the device's "*digital* inner workings" as this search "is only incidentally connected to the physical place where the search is being conducted."[205] CBP maintains that "[searches of electronic devices] are part of CBP's longstanding practice and are essential to enforcing the law at the U.S. border and to protecting border security."[206] However, imposing a standard that requires border agents to demonstrate reasonable suspicion would pose virtually no national security risks because, while undesirable, digital contraband such as child pornography does not implicate the physical and imminent threats to national security contemplated at the adoption of the border

201. United States v. Seljan, 547 F.3d 993, 1015 (9th Cir. 2008) (Kozinski, C.J., dissenting).

202. *Id.* (citing United States v. Bulacan, 156 F.3d 963, 967 (9th Cir. 1998)).

203. Rankin, *supra* note 7, at 347 (arguing that attorneys may have privileged information on their electronic devices, international students may experience interference with their studies due to delay resulting from their devices being seized, and "other law-abiding citizens" will be subjected to a serious invasion of privacy as "their most private emails, photographs, financial data, and other effects" are searched).

204. Wilson, *supra* note 177, at 1013 (arguing that "[o]ther than the location where the search would take place, the search of laptop files has little to do at all with the borders; there is nothing exceptional or dangerous about information, ideas, and data being physically carried across the border on a hard drive that makes it more reasonable to search than the same data, located on the same hard drive, on your desk at home.").

205. Rechtin, *supra* note 18, at 89.

206. *See* U.S. CUSTOMS & BORDER PROTECTION, CBP DIRECTIVE NO. 3340-049A, BORDER SEARCH OF ELECTRONIC DEVICES at 1 (2018), https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Eiectronic-Media-Compliant.pdf [https://perma.cc/LCH9-3NCJ].

search doctrine.[207] Moreover, requiring a showing of reasonable suspicion would not impede "legitimate law enforcement objectives" because reasonable suspicion is not a "high threshold" to meet.[208]

F. Imposition of an Even Higher Standard: Probable Cause Required?

While reasonable suspicion is the most stringent standard ever applied to searches at the border,[209] perhaps it is necessary to require a showing of probable cause where forensic searches of electronic devices are involved. Some commentators go further, suggesting the government should be required to obtain a *warrant* before performing forensic searches at the border.[210] Arguably, imposing this requirement for searches of digital data would not interfere with the government's national security interests—border agents remain free to search for physical contraband, such as weapons, that may pose an imminent danger.[211] Further, anything less than probable cause may fail to afford enough protection to a traveler's privacy; under the current state of the law, international travelers "should not expect much" when it comes to their digital devices.[212]

VI. CONCLUSION

The border search exception is justified on the basis of the government's interest in national security, which has been recognized as

207. *See* Wright, *supra* note 165, at 728 (arguing that "the purpose of the border search exception to the Fourth Amendment was to prevent the entry of physical contraband into the United States" and that files contained on a computer should not fall into the same category as contraband such as "firearms" and "controlled substances (drugs)" for the purpose of Fourth Amendment protection).

208. Rankin, *supra* note 7, at 340–42.

209. United States v. Wanjiku, 919 F.3d 472, 481 (7th Cir. 2019) (citing United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985)).

210. *See, e.g.*, Christopher I. Pryby, Note, *Forensic Border Searches After Carpenter Require Probable Cause and a Warrant*, 118 Mich. L. Rev. 507, 509 (2019) (arguing the government should be required to show both probable cause and obtain a warrant prior to forensically searching a traveler's electronic device).

211. *Id.* at 526.

212. *See* 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, 102–03 (2016) (arguing that it is more likely border agents will find "incriminating evidence" when searching an electronic device as opposed to a suitcase, and without requiring border agents to show probable cause before undertaking a search, the border search doctrine could be easily exploited).

greatest at the border.[213] However, travelers should not be required to relinquish all constitutional rights simply by virtue of traveling internationally, especially considering a traveler's increased privacy expectations that have come with modern technology.[214] The current suspicionless standard inadvertently allows customs agents to search devices for a variety of "bad reasons."[215] Accordingly, the Supreme Court will soon need to establish a uniform standard with respect to forensic searches of electronic devices at the border.[216] Alternatively, Congress could set an appropriate standard.[217]

The uniquely intrusive nature of forensic searches makes it inappropriate to classify them as "routine," placing the search of an electronic device in the same category as that of a suitcase or other traditional container.[218] The constitutional protections afforded by the Fourth Amendment should not be forgotten solely because an individual chooses to cross the border.[219] Where electronic data is the subject of a search, there is "enormous potential for a violation of the owner's expectation of privacy."[220] Accordingly, some degree of particularized suspicion should be required before federal agents can perform forensic searches despite the physical location at which the search occurs.

While the Supreme Court has not identified what, exactly, renders a search "nonroutine,"[221] forensic searches should be placed into this category, requiring border agents to possess individualized suspicion

213. United States v. Flores-Montano, 541 U.S. 149, 152 (2004).

214. United States v. Cotterman, 709 F.3d 952, 965–66 (9th Cir. 2013) (noting that while a traveler may not feel his privacy has been violated if law enforcement searches his briefcase, he may feel a greater intrusion where his laptop is searched "due to the vast amount of information potentially available on electronic devices.").

215. Ari B. Fontecchio, *Suspicionless Laptop Searches Under the Border Search Doctrine: The Fourth Amendment Exception That Swallows Your Laptop*, 31 CARDOZO L. REV. 231, 264–65 (2009) (arguing that border officers should not conduct a search based solely on the officer's "hunch" or racial profiling, and searches should not be conducted for the purpose of "harassing a bothersome traveler" and that a suspicionless standard "allows searches for all these bad reasons, compromising efficiency and border security."). The author recommends a "one good reason" standard, which would prohibit border agents from conducting forensic searches of electronics at the border unless the officer had "one good reason" for doing so, as this would ensure that the search was directed at detecting "harmful data." *Id.* at 256.

216. 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, 312 (2017).

217. Bector, *supra* note 13, at 717.

218. Rachel Flipse, Comment, *An Unbalanced Standard: Search & Seizure of Electronic Data Under the Border Search Doctrine*, 12 U. PA. J. CONST. L. 851, 862 (2010).

219. *Id.* at 863.

220. *Id.*

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

before forensically searching a traveler's device.[222] As the Fourth Circuit explained in *Kolsuz*, forensic searches should be categorized as nonroutine based on the "sheer quantity of data" capable of being stored on digital devices and the "uniquely sensitive nature" of the information stored.[223] Forensic searches are significantly more intrusive than the search of other types of property.[224]

Further, electronic devices should be treated as distinct from mere containers.[225] The storage capacity of traditional containers is far exceeded by that of modern electronic devices, and one commentator noted that "one hard drive may hold the paper equivalent of more than twice the number of trees in Central Park."[226] While the search of a traditional "container" such as a suitcase has the potential to reveal sensitive personal information, "it does not in the process transmit the *whole* of a person's life."[227] While a suitcase and cell phone are both used for storage, they have distinct functions in our modern world and should be treated differently for the purpose of the Fourth Amendment—even at the border.

As an alternative to the current suspicionless standard, forensic searches at the border should require, at a minimum, a showing of reasonable suspicion.[228] A reasonable suspicion standard is only a "minimal requirement, just the next level up from no suspicion at all," and it is unlikely that imposition of such a standard would create any substantial risk to national security.[229] Some commentators advocate for an even a higher standard, arguing that a showing of probable cause is necessary to prevent federal agents from bypassing Fourth Amendment

222. O'Grady, *supra* note 47, at 2260 (advancing the proposition that "all border searches of electronic devices are therefore nonroutine and require some form of individualized suspicion.").

223. *Kolsuz*, 890 F.3d at 144–45.

224. United States v. Cotterman, 709 F.3d 952, 966 (9th Cir. 2013) ("[T]he exposure of confidential and personal information has permanence. It cannot be undone. Accordingly, the uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy and thus renders and exhaustive exploratory search more intrusive than with other forms of property.").

225. Leach, *supra* note 186, at 329 (arguing that electronic devices may present a "new category of property" for the purpose of evaluating protection under the Fourth Amendment, as electronic devices are different from "a closed container or a vehicle.").

226. Maddalena DeSimone, Note, *Can We Curate It? Why Luggage and Smartphones Merit Different Treatment at the United States Border*, 2019 Colum. BUS. L. REV. 696, 726 (2019).

227. Donohue, *supra* note 31, at 1010.

228. *Cotterman*, 709 F.3d at 966 ("Reasonable suspicion is a modest, workable standard that is already applied in the extended border search, *Terry* stop, and other contexts. Its application to the forensic examination here will not impede law enforcement's ability to monitor and secure our borders or to conduct appropriate searches of electronic devices.").

229. O'Grady, *supra* note 47, at 2283.

requirements by choosing to simply "wait for their suspect to arrive at the border" to search her devices.[230] Border agents should not be afforded access to "a loophole to Fourth Amendment protections" for searches that fail to further the recognized purpose of the border search exception: national security.[231]

If a traveler does not want to subject any items of personal property to search, he can choose to leave those items at home rather than packing them in his suitcase. The same cannot be said about electronic devices,[232] especially the modern cell phone, which arguably is not "optional" when an individual chooses to travel internationally.[233] Thus, suspicionless searches of digital information at the border may infringe upon on an individual's right to travel.[234] Whether reasonable suspicion or something more, a consistent standard requiring some degree of suspicion for forensic searches at the border must be instituted to protect the privacy expectations of unsuspecting travelers and the security of our great nation.

230. Park, *supra* note 216, at 296. *See also* Bohannon, *supra* note 152, at 599 ("In other cases, where an individual is suspected of a crime, the government has used the border search authority of CBP to access information or records the agency would not otherwise have access to if they were inside the country, even where the investigation is for a crime unrelated to the individual's international travel, customers laws, immigration, or terrorism.").

231. Bohannon, *supra* note 152, at 599.

232. Because deleted information may be accessible during a search of an electronic device, travelers are not able to "choose what they bring with them and what they leave at home" in the same way they could choose what to place in their luggage. Samuel Townsend, *Laptop Searches at the Border and United States v. Cotterman*, 94 B.U. L. REV. 1745, 1764 (2014).

233. Donohue, *supra* note 31, at 1004, 1007 (noting that most travelers that enter or exit the country bring their devices "to satisfy a host of logistical and recreational needs" and often "need their devices once they reach their destination."). *See also* United States v. Saboonchi, 990 F. Supp. 2d 536, 557–58 (D. Md. 2014) (characterizing "mobile devices" 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, and, particularly, of traveling to unstable or dangerous regions of the world.").

234. Nathan Alexander Sales, *Run for the Border: Laptop Searches & the Fourth Amendment*, 43 U. RICH. L. REV. 1091, 1100–01 (2009) (travelers may choose not to travel at all out due to "fear that customs officers will rifle through their electronic data.").