Electronic Searches at the Border: Reasonable Suspicion or None at All? The Circuit Split and Potential Impact on Higher Education

"It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[1]

I. INTRODUCTION

In August 2019, U.S. Customs and Border Protection (CBP) detained Ismail Ajjawi, a seventeen-year-old incoming Harvard College student from Palestine, after he arrived in the United States at Boston's Logan Airport.[2] After hours of questioning and an extensive search of Ajjawi's cell phone and computer, CBP revoked Ajjawi's visa and denied him entry into the United States.[3] Harvard University, along with select advocacy groups, fought the visa denial on Ajjawi's behalf, and ten days later, the Department of Homeland Security (DHS) permitted Ajjawi to enter the United States.[4]

Ajjawi's situation is not uncommon, as the search and seizure of electronic devices at U.S. borders has increased each year.[5] The rise in electronic border searches underscores the need for a definitive standard of suspicion to permit border agents to conduct these searches.[6] Without a clear standard, travelers' rights are at risk, and over one million international students in the United States

---

1. Kyllo v. United States, 533 U.S. 27, 33-34 (2001).

2. *See* Susan Svrluga, *Palestinian Student Originally Denied Entry to U.S. Now Allowed in to Attend Harvard*, WASH. POST (Sept. 3, 2019, 4:00 PM), https://www.washingtonpost.com/education/2019/09/03/palestinian-student-originally-denied-entry-us-now-allowed-attend-harvard/ [https://perma.cc/DLG7-8Q48] (detailing story of incoming Harvard student detained at airport).

3. *See* Caitlin Dickson, *Outrage Mounts over Harvard Student Turned Back at Airport*, YAHOO NEWS (Aug. 28, 2019), https://news.yahoo.com/outrage-mounts-over-harvard-student-turned-back-at-airport-after-cell-phone-search-222753962.html [https://perma.cc/222P-CMJR] (describing international student's entry denied after search of cell phone and computer).

4. *See* Svrluga, *supra* note 2 (detailing student's subsequent entry into United States).

5. *See* Press Release, Dep't of Homeland Sec., U.S. Customs & Border Prot., CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics (Jan. 5, 2018), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and [https://perma.cc/B5P6-2PV8] [hereinafter CBP FY17 Statistics] (displaying increased incidents of electronic searches at border from 2016 to 2017). According to CBP statistics, the number of electronic device searches by border agents nearly tripled in October 2017 as compared to October 2016. *See id.*

6. *See* Laura Nowell, Note, *Privacy at the Border: Applying the Border Search Exception to Digital Searches at the United States Border*, 71 FED. COMMC'NS L.J. 85, 87 (2018) (explaining need for clarity regarding level of suspicion for border searches).

risk being turned away at the border as they enter each year or return from school vacations.[7] This uncertainty not only jeopardizes international students' educational opportunities, but also threatens the higher education system's reliance on the income and diversity contributed by international students.[8]

Individuals in the United States have an expectation of privacy against unreasonable searches and seizures by government officials.[9] This expectation is grounded in the Fourth Amendment, which protects against such intrusions.[10] Further, the Fourth Amendment requires law enforcement to obtain a search warrant based on probable cause as warrantless searches and seizures are per se unreasonable, subject to certain exceptions.[11]

One of the earliest recognized exceptions to the Fourth Amendment's warrant requirement is the border search exception, which allows officers at the border, or "its functional equivalent," to conduct "reasonable" searches of persons and property without a warrant or probable cause.[12] The United States Supreme

---

7. *See* INST. OF INT'L EDUC., OPEN DOORS FAST FACTS 2010-2019, at 17 (2019), https://opendoorsdata.org/wp-content/uploads/2020/11/Open-Doors-Fast-Facts-2010-2019.pdf [https://perma.cc/L8HZ-KRNG] (reporting 1,094,792 international students in United States for 2017-2018 school year); Dickson, *supra* note 3 (stating CBP has authority to revoke visa based on search at border); *infra* Section II.E (presenting impact on international students). While the State Department issues and revokes visas, CBP makes the final decision on entry once an individual arrives at the border because CBP can cancel an individual's visa at the border based on information discovered during the border inspection. *See* Dickson, *supra* note 3. Further, legal experts are concerned that Ajjawi's situation highlights the "increasingly common practice of searching travelers' electronic devices and using social media to vet visa applicants." *Id.*

8. *See* NAFSA, THE UNITED STATES OF AMERICA: BENEFITS FROM INTERNATIONAL STUDENTS (2020), https://www.nafsa.org/sites/default/files/media/document/isev-2020.pdf [https://perma.cc/46LP-SK8N] (reporting international students contributed almost $39 billion to higher education in 2019-2020 academic year); Laura McKenna, *The Globalization of America's College*s, THE ATL. (Nov. 18, 2015), https://www.theatlantic.com/education/archive/2015/11/globalization-american-higher-ed/416502/ [https://perma.cc/DH8D-UYU9] (describing international students' impact on diversity in U.S. higher education). Additionally, NAFSA reported that international students supported more than 415,000 jobs in the United States in the 2019-2020 academic year. NAFSA, *supra*. While international students comprise only 5.5% of enrolled students in U.S. higher education, their financial contributions are significant and something many universities have come to depend on. Karin Fischer, *Higher Education Is in Trouble, and Not Just Because of the Coronavirus*, WORLD POL. REV. (Oct. 13, 2020), https://www.worldpoliticsreview.com/articles/29129/with-the-coronavirus-higher-education-suffers-enormous-losses [https://perma.cc/HAE2-ELZB] (detailing international students' financial contributions to U.S. higher education). Their financial contributions are significant because most international students pay the full cost of their degree or close to it, and, unlike American students, do not receive much financial aid. *See id.*

9. *See* U.S. CONST. amend. IV (establishing protection from unreasonable searches and seizures).

10. *See id.*

11. *See id.* (stating "no warrants shall issue, but upon probable cause"); JEANETTE DORAN BROOKS, INST. OF GOV'T, VALID SEARCHES AND SEIZURES WITHOUT WARRANTS 1-8 (2004), http://www.ncids.org/Defender%20Training/2004%20Fall%20Conference/Exceptions.pdf [https://perma.cc/23MG-MW3K] (listing different exceptions to warrant requirement). The exceptions to the warrant requirement include exigent circumstances, search incident to arrest, vehicle searches, consent searches, border searches, open fields, plain view, and special needs. *See* BROOKS, *supra*, at 1-8; *see also* 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, 554 & n.3 (2019) (noting several exceptions to warrant requirement).

12. *See* United States v. Ramsey, 431 U.S. 606, 616-17 (1977) (detailing extensive history of border search exception); *see also* Sean O'Grady, Note, *All Watched Over by Machines of Loving Grace: Border Searches of*

Court has consistently justified suspicionless and warrantless searches at the border by reasoning that the government has an interest in controlling "who and what may enter the country."[13] In *Riley v. California*,[14] the Court addressed the constitutionality of warrantless searches of electronic devices incident to a lawful arrest.[15] The Court, however, has not addressed the growing concern over suspicionless searches of electronic devices at the border, leading to the current circuit split and inconsistency in application of the exception.[16] The Fourth and Ninth Circuits both held that forensic searches of electronic devices at the border require some level of individualized suspicion, whereas the Eleventh Circuit held that no level of suspicion is required.[17] This inconsistent application of the border search exception could have a lasting impact on the diversity and financial well-being of the United States' higher education system.[18]

This Note examines the border search exception to the Fourth Amendment, the circuit split regarding its applicability to the search and seizure of electronic devices, and the exception's potential impact on higher education in the United States.[19] Part II provides a brief history of the Fourth Amendment and its application to electronic searches as set out in *Riley v. California*, the historical context and an overview of the border search exception, an overview of the circuit split regarding the applicability of *Riley* to digital searches at the border, and a

---

Electronic Devices in the Digital Age, 87 FORDHAM L. REV. 2255, 2257, 2262-63 (2019) (discussing border search exception history). The "functional equivalent" of the U.S. border includes international airports. *See* O'Grady, *supra*, at 2263 & n.61.

13. *See Ramsey*, 431 U.S. at 620 (explaining rationale behind border search exception); *see also* United States v. Flores-Montano, 541 U.S. 149, 153 (2004) (providing history of Court's justification for border exception); O'Grady, *supra* note 12, at 2257 (describing historical justification of exception by Court).

14. 573 U.S. 373 (2014).

15. *Id.* at 403 (holding warrantless search of cell phone unconstitutional and violation of Fourth Amendment).

16. *Compare* United States v. Kolsuz, 890 F.3d 133, 144 (4th Cir. 2018) (holding some level of individualized suspicion necessary for forensic search of electronic devices), *with* United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013) (en banc) (holding reasonable suspicion required for forensic search of electronic devices). The Fourth Circuit followed the Supreme Court's holding in *Riley* and applied it to searches at the border; the Ninth Circuit undertook a similar analysis in a pre-*Riley* case. *See Kolsuz*, 890 F.3d 133 at 144; *Cotterman*, 709 F.3d at 956-57. *But see* United States v. Touset, 890 F.3d 1227, 1229 (11th Cir. 2018) (holding no suspicion required for forensic searches of electronic devices). The First Circuit recently joined the Eleventh Circuit, holding that advanced searches of electronic devices do not require a warrant or probable cause, and joined the Ninth and Eleventh Circuits in further holding that basic searches of electronic devices do not require reasonable suspicion. *See* Alasaad v. Mayorkas, 988 F.3d 8, 13 (1st Cir. 2021).

17. *See supra* note 16 and accompanying text (describing circuit split).

18. *See* Alia Wong, *Colleges Face Growing International Student-Visa Issues*, THE ATL. (Sept. 6, 2019), https://www.theatlantic.com/education/archive/2019/09/how-harvard-and-other-colleges-grapple-student-visa-problems/597409/ [https://perma.cc/R5VQ-K735] (detailing higher education concerns regarding visa revocation). Although foreign nationals with U.S. visas are subject to searches at the U.S. border, they may not have the same constitutional protections as U.S. citizens and non-citizens with connections to the United States. *See* Atanu Das, *Chilling Social Media: Warrantless Border Searches of Social Media Accounts Infringe upon the Freedom of Association and the Freedom to Be Anonymous Under the First Amendment*, 84 BROOK. L. REV. 1287, 1295-96 (2019).

19. *See infra* Parts II-IV.

discussion of the role international students play in the U.S. higher education system.[20] Part III analyzes the impracticability of a strict application of *Riley* and argues that reasonable suspicion is the appropriate standard for electronic searches at the border.[21] Finally, Part IV recommends that the Court adopt the reasonable suspicion standard for forensic searches of electronic devices at the border to preserve travelers' rights to privacy as well as the financial well-being of the higher education system, while still protecting the heightened governmental interest at the border.[22]

II. HISTORY

A. The Fourth Amendment Right to Privacy

The Fourth Amendment provides that:

> 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.[23]

The Amendment does not establish a "general constitutional 'right to privacy,'" and as a result, determining when these protections apply causes constant litigation.[24] In his concurring opinion in *Katz*, Justice Harlan established the two-part test used to determine whether a government action constitutes a search that

20. *See infra* Part II.

21. *See infra* Part III.

22. *See infra* Part IV.

23. U.S. CONST. amend. IV.

24. *See* Katz v. United States, 389 U.S. 347, 350-51 (1967) (explaining context of Fourth Amendment's application); Thomas Mann Miller, Comment, *Digital Border Searches After* Riley v. California, 90 WASH. L. REV. 1943, 1951 (2015) (describing structure of Fourth Amendment analysis); Brent E. Newton, *The Real-World Fourth Amendment*, 43 HASTINGS CONST. L.Q. 759, 760-61 (2016) (noting Fourth Amendment issues most common before Court). The Fourth Amendment is not a "general constitutional 'right to privacy'"; it protects against specific forms of governmental intrusions, as set out in its text, but no more. *Katz*, 389 U.S. at 350. A person's general right to privacy, or the right to be left alone by others, is primarily left to the states. *See id.* at 350-51. Further, the Fourth Amendment only applies to government officials and not to individual citizens. *See* United States v. Jacobsen, 466 U.S. 109, 115 (1984) (holding search of package by private party not violation since not requested by government official); Newton, *supra*, at 760 & n.1 (describing limits and applicability of Fourth Amendment protections). Many judicial opinions and scholarly articles refer to the Fourth Amendment as protecting the rights of "citizens" rather than "the people" as the Fourth Amendment's language states. *See* M. Isabel Medina, *Exploring the Use of the Word "Citizen" in Writings on the Fourth Amendment*, 83 IND. L.J. 1557, 1557 (2008) (describing use of "citizen" misleading and concerning).

triggers Fourth Amendment protections.[25] This inquiry is both subjective and objective and is often referred to as the "reasonable expectation of privacy" test.[26]

Under this test, the government action must invade an individual's privacy interest protected by the Fourth Amendment, and the individual must exhibit an "actual (subjective) expectation of privacy."[27] Next, the individual's expectation must be "one that society is prepared to recognize as 'reasonable.'"[28] If a court finds that a government action constituted a search—i.e., an invasion of an individual's "reasonable expectation of privacy"—then the court must determine whether the search or seizure was reasonable.[29]

Generally, a search is reasonable if it is accompanied by a valid warrant supported by probable cause.[30] A search or seizure executed without a judicial warrant or showing of probable cause is per se unreasonable.[31] Additionally, courts often deem a search unreasonable when no "individualized suspicion of

25. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring) (articulating two-fold requirement emerging from prior decisions); *see also* Byrd v. United States, 138 S. Ct. 1518, 1526 (2018) (describing primacy of Harlan's test and "most often associated with legitimate expectations of privacy"); Kyllo v. United States, 533 U.S. 27, 33 (2001) (applying Justice Harlan's two-part inquiry); 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, 703-04 (2019) (describing two-part inquiry in *Katz* and subsequent Supreme Court adoption).

26. *See* Bond v. United States, 529 U.S. 334, 338 (2000) (describing two questions embraced in Fourth Amendment analysis); DeSimone, *supra* note 25, at 704 (describing subjective and objective nature of inquiry); Miller, *supra* note 24, at 1951 (naming Fourth Amendment privacy test courts use).

27. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring) (setting out first part of inquiry); *see also* Miller, *supra* note 24, at 1951 (explaining privacy interest must have Fourth Amendment protection). The Court has held that an individual has a reasonable expectation of privacy in several areas, even those where an individual does not have a common law property interest in the place searched. *See* DeSimone, *supra* note 25, at 705-06 (identifying sub-spheres where Court has found reasonable expectations of privacy); *see also Byrd*, 138 S. Ct. at 1531 (holding driver in lawful possession of rental car has reasonable expectation of privacy); Florida v. Jardines, 569 U.S. 1, 7 (2013) (holding front porch of home extension of residence requiring warrant for search); *Bond*, 529 U.S. at 338-39 (holding bus passenger's expectation of privacy for carry-on bag reasonable); Michigan v. Clifford, 464 U.S. 287, 297 (1984) (holding reasonable expectation of privacy in fire-damaged residence). *But see* California v. Ciraolo, 476 U.S. 207, 213-14 (1986) (holding no reasonable expectation of privacy in air space above residence).

28. *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (describing objective nature of second prong).

29. *See id.*; Riley v. California, 573 U.S. 373, 381-82 (2014) (discussing reasonableness requirement of Fourth Amendment). The Court stated that it is clear that "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'" *Riley*, 573 U.S. at 381-82 (quoting Brigham City v. Stuart, 547 U.S. 398, 403 (2006)); *see* Gina R. Bohannon, Comment, *Cell Phones and the Border Search Exception: Circuits Split over the Line Between Sovereignty and Privacy*, 78 MD. L. REV. 563, 566 (2019) (discussing steps courts must take to determine Fourth Amendment violation).

30. *See Riley*, 573 U.S. at 382 (stating reasonable search or seizure generally requires judicial warrant); Bohannon, *supra* note 29, at 566 (describing presumption of reasonableness for warrants supported by probable cause).

31. *See* United States v. Place, 462 U.S. 696, 701 (1983) (noting ordinary circumstances where Court held searches unreasonable); O'Grady, *supra* note 12, at 2261 (discussing what constitutes reasonable search).

wrongdoing" exists.[32] Nevertheless, a search or seizure is reasonable absent a warrant if it falls within one of the well-established exceptions.[33]

These exceptions to the warrant requirement apply to searches and seizures in situations where law enforcement has special needs, the individual has a diminished expectation of privacy, or where the search and seizure effectuates a minimal intrusion.[34] Because "the Fourth Amendment's ultimate touchstone is 'reasonableness,'" even the exceptions are based on reasonableness.[35] For a search or seizure conducted pursuant to an exception to be reasonable, the nature and degree of the intrusion must be balanced against "the importance of the governmental interests alleged to justify the intrusion."[36] Additionally, even in these limited circumstances, the Court generally requires that the search or seizure pursuant to the underlying exception is supported by probable cause, or at least reasonable suspicion, in order to permit the warrantless search or seizure that follows.[37] The border search exception, however, generally does not require any level of individualized suspicion for routine searches.[38]

---

32. *See* City of Indianapolis v. Edmond, 531 U.S. 32, 37 (2000) (restating Fourth Amendment principle requiring individualized suspicion). While individualized suspicion is generally a prerequisite for a reasonable search and seizure, "the Fourth Amendment imposes no irreducible requirement of such suspicion" and there are limited circumstances where this requirement does not apply. United States v. Martinez-Fuerte, 428 U.S. 543, 560-61 (1976) (detailing certain exceptions to requirement of individualized suspicion).

33. *See* Katz v. United States, 389 U.S. 347, 357 (1967); *Stuart*, 547 U.S. at 403 (recognizing exigent circumstances exception); Horton v. California, 496 U.S. 128, 135 (1990) (applying plain view exception to warrant requirement); United States v. Ramsey, 431 U.S. 606, 617 (1977) (reaffirming border search exception); Agnello v. United States, 269 U.S. 20, 30 (1925) (holding search incident to lawful arrest exception to warrant requirement); *supra* note 11 and accompanying text (noting Fourth Amendment warrant requirement and exceptions to requirement).

34. Illinois v. McArthur, 531 U.S. 326, 330 (2001); *see* Allison M. Lucier, Comment, *You Can Judge a Container by Its Cover: The Single-Purpose Container Exception and the Fourth Amendment*, 76 U. CHI. L. REV. 1809, 1812 (2009) (citing types of exceptions to warrant requirement).

35. *See, e.g.*, Brigham City v. Stuart, 547 U.S. 398, 403-04 (2006) (applying warrant exception but engaging in reasonableness analysis); *see also* Bohannon, *supra* note 29, at 566 (noting some searches reasonable absent warrant if acting under exception).

36. *Place*, 462 U.S. at 703; *see* Bohannon, *supra* note 29, at 566 (describing balancing test courts apply).

37. *See* Ker v. California, 374 U.S. 23, 34-35 (1963) (requiring probable cause for search incident to lawful arrest); Terry v. Ohio, 392 U.S. 1, 27 (1968) (requiring reasonable suspicion for investigatory stop). Probable cause under the search incident to lawful arrest exception exists "where 'the facts and circumstances within [the officers'] knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that' an offense has been or is being committed." *Ker*, 374 U.S. at 34-35 (quoting Brinegar v. United States, 338 U.S. 160, 175-76 (1949)); *see* United States v. Arvizu, 534 U.S. 266, 273 (2002) (stating government interests favor standard lower than probable cause with brief investigatory stops); *Terry*, 392 U.S. at 27 (holding brief investigatory stop constitutional with reasonable suspicion). Reasonable suspicion is a lower standard than probable cause, but still "requires at least a minimal level of objective justification for making the stop." Illinois v. Wardlow, 528 U.S. 119, 123 (2000). The officer or government official must have more than an "inchoate and unparticularized suspicion or 'hunch'" of criminal activity. *Terry*, 392 U.S. at 27.

38. *See Ramsey*, 431 U.S. at 616-19 (delineating history and purpose of exception); Miller, *supra* note 24, at 1953 (noting no probable cause or reasonable suspicion requirement for border search exception); *see also infra* Section II.B.2 (differentiating between routine and nonroutine searches). Individualized suspicion is an integral component of probable cause and "is the idea that the state should judge each citizen based upon his own unique actions, character, thoughts, and situation . . . [and not on] stereotypes, assumptions, guilt-by-association,

B. The Border Search Exception

1. History of Border Search Exception

The border search exception is one of the oldest recognized exceptions to the warrant requirement.[39] The same Congress that proposed the Bill of Rights—including the Fourth Amendment—passed the Act of July 31, 1789 (Act).[40] The Act, the first customs statute in the United States, "granted customs officials 'full power and authority' to enter and search 'any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed'" without a warrant or probable cause.[41] The Act distinguishes between searches at the border and searches in homes, buildings, or other dwelling places within the interior of the country.[42] This distinction highlights the border search exception's rationale, which is "grounded in the recognized right of the sovereign to control . . . who and what may enter the country" and on the understanding that individuals have a diminished expectation of privacy at the border.[43] The Supreme Court has relied on the exception's "impressive historical pedigree" in continually upholding the constitutionality of warrantless searches at the border.[44]

In the twentieth century, as Fourth Amendment jurisprudence continued to evolve, the border exception did as well.[45] The Court laid the initial groundwork

---

or other generalities." Andrew E. Taslitz, *What Is Probable Cause, and Why Should We Care?: The Costs, Benefits, and Meaning of Individualized Suspicion*, 73 LAW & CONTEMP. PROBS., Summer 2010, at 145-46.

39. *See* O'Grady, *supra* note 12, at 2262 (describing interconnection of border exception and Act of July 31, 1789); Rasha Alzahabi, Note, *Should You Leave Your Laptop at Home When Traveling Abroad?: The Fourth Amendment and Border Searches of Laptop Computers*, 41 IND. L. REV. 161, 166 (2008) (describing border search exception dating to First Congress).

40. *See* Act of July 31, 1789, ch. 5, § 24, 1 Stat. 29, 43 (repealed 1790) (providing warrantless authority for U.S. customs officials to search for illegal goods at checkpoints), https://www.loc.gov/law/help/statutes-at-large/1st-congress/c1.pdf [https://perma.cc/8ZMJ-B3T9]; *see also* United States v. Ramsey, 431 U.S. 606, 616 (1977) (describing historical context of originally adopted border exception).

41. § 24, 1 Stat. at 43; *see Ramsey*, 431 U.S. at 616 (providing history of exception).

42. *See* §§ 23-24, 1 Stat. at 43 (distinguishing between different searches); Bohannon, *supra* note 29, at 571 (noting Act's distinction between searches at border and those in dwelling places).

43. *Ramsey*, 431 U.S. at 620; *see* United States v. Flores-Montano, 541 U.S. 149, 154 (2004) (acknowledging lower expectation of privacy at border than interior). This distinction in privacy expectations exists in part because "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *Flores-Montano*, 541 U.S. at 152.

44. United States v. Villamonte-Marquez, 462 U.S. 579, 585 (1983); *see Ramsey*, 431 U.S. at 616-17 (describing historical importance of enactment of border exception by same Congress that enacted Fourth Amendment). The Act of July 31, 1789 was passed two months prior to the proposal of the Bill of Rights. *See Ramsey*, 431 U.S. at 616. The Court has interpreted this temporal closeness as evidence of the First Congress's intent in preserving the border search exception and its recognition of the heightened government interest at the border. *See* Boyd v. United States, 116 U.S. 616, 623 (1886). In *Boyd*, the Court noted, "it is clear that the members of that body did not regard searches and seizures of this kind as 'unreasonable,' and they are not embraced within the prohibition of the amendment." *Id.*

45. *See* Atanu Das, *Crossing the Line: Department of Homeland Security Border Search of Mobile Device Data Likely Unconstitutional*, 22 U. PA. J.L. & SOC. CHANGE 205, 216 (2019) (describing evolution of Fourth Amendment jurisprudence).

for the modern border search exception doctrine in *Carroll v. United States*.[46] There, the Court distinguished between automobile searches at the U.S. border and those searches occurring within the United States.[47] The Court held that warrantless searches of vehicles within the border are permitted as long as they are supported by probable cause.[48] In coming to its decision, the Court used the border search exception as a point of comparison stating, "[t]ravelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in."[49] This language laid the groundwork for the modern border search exception.[50]

Following *Carroll*, the Supreme Court specifically addressed the border search exception in three seminal cases: *United States v. Ramsey*, *United States v. Montoya de Hernandez*, and *United States v. Flores-Montano*.[51] While the Court mentioned the border search exception in previous cases, *Ramsey* is the first case in which the Court expressly ruled on the exception.[52] In *Ramsey*, customs officials invoked the border search exception to conduct a warrantless search of envelopes that had arrived in the mail from Thailand.[53] The customs officials suspected that the envelopes contained narcotics based on their unusual bulkiness and weight, as well as their country of origin.[54] The Court upheld the search of the envelopes and ruled that the customs official had "reasonable 'cause

46. *See* Carroll v. United States, 267 U.S. 132, 154 (1925) (analyzing context of border search exception); *see also* Das, *supra* note 45, at 216 (noting modern border exception first promulgated in *Carroll*); WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 10.5(a) (5th ed. 2019) (stating Court had no occasion to opine directly on border exception before *Carroll*).

47. *See Carroll*, 267 U.S. at 154 (distinguishing between searches at border and within United States); Bohannon, *supra* note 29, at 572 (noting importance of distinction and language in *Carroll*).

48. *See Carroll*, 267 U.S. at 153-54 (holding warrantless searches of vehicles permitted when accompanied by probable cause). The Court reasoned that securing a warrant to search a vehicle, boat, ship, or wagon is not always practical because the suspect can easily move them out of the jurisdiction where the warrant is sought, justifying the exception. *Id.* at 153.

49. *Id.* at 153-54 (articulating Court's reasoning).

50. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 563 (1985) (Stevens, J., concurring) (citing *Carroll* language); United States v. Ramsey, 431 U.S. 606, 617-18 (1977) (recognizing language in *Carroll* set groundwork for border search exception); Will Carroll, Note, *"Please Unlock Your Phone": Why Reasonable Suspicion Should Be Extended to Cursory Searches of Electronic Devices at the Border*, 107 KY. L.J. ONLINE 1, 4 (2018), https://static1.squarespace.com/static/5d28bbdff1b73800019f9a52/t/5dc9f63e344d941b579f09ec/1573516862439/Nash+Note+Final.pdf [https://perma.cc/JQ7X-5K2A] (noting importance of language in *Carroll* and Court's later reliance).

51. *See* Miller, *supra* note 24, at 1954 (listing Supreme Court cases addressing border search exception); United States v. Flores-Montano, 541 U.S. 149, 152 (2004); *Montoya de Hernandez*, 573 U.S. at 540; *Ramsey*, 431 U.S. at 611.

52. *See* Miller, *supra* note 24, at 1954 (noting Court's first direct ruling on border search exception in *Ramsey*).

53. *See Ramsey*, 431 U.S. at 609-10 (detailing circumstances in case).

54. *See id.* at 609 (describing unusual weight and appearance of envelopes); *see also* Das, *supra* note 45, at 217 (outlining case facts).

to suspect'" that the envelopes contained contraband.[55] In *Ramsey*, the Court established that routine searches of persons and property at the border are reasonable "by virtue of the fact that they occur at the border," due to the sovereign's strong interest in controlling "who and what may enter the country."[56] Importantly, the Court expressly reserved the question of "whether, and under what circumstances, a border search might be deemed 'unreasonable' because of the particularly offensive manner in which it is carried out."[57]

2. Routine Versus Nonroutine Searches at the Border

A border search's presumptive reasonableness is not absolute.[58] The Court has not developed a bright-line rule because reasonableness, especially in the context of a border search, "is incapable of comprehensive definition or of mechanical application."[59] Instead, the Court stressed the need for a case-by-case analysis of whether a border search is reasonable.[60] To assist in this difficult analysis, the Court has created two general categories of border searches—"routine" and "nonroutine."[61]

A "routine" border search is one that does not "pose a serious invasion of privacy and that [does] not embarrass or offend the average traveler."[62] Routine searches at the border do not require any level of suspicion of criminal activity

---

55. *See Ramsey*, 431 U.S. at 614-15, 624-25 (upholding warrantless search made under postal statute). The Court differentiated between contraband inside a letter and the actual correspondence but did not find it necessary to address the potential First Amendment consequences of reading the correspondence within the letter. *See id.* at 624. The Court reasoned such analysis was unnecessary because the officer had reason to believe, based on the bulkiness and weight of the envelopes, that they contained something other than correspondence. *See id.* at 614-15 (holding officer's suspicions valid statutory reason for opening envelopes). Additionally, the customs officials found heroin in the envelope; therefore, the correspondence within the letter was never at issue. *See id.* at 609-10. Importantly, the Court did not grant broad power to search any mailed correspondence without probable cause or a warrant, but only when the officer has "reasonable cause to believe" there is contraband. *See id.* at 623; *see also* Miller, *supra* note 24, at 1955-56 (emphasizing *Ramsey* Court's limited holding).

56. United States v. Ramsey, 431 U.S. 607, 616, 620 (1977) (establishing modern application of border search exception). The Court, however, noted that the right to control who and what may enter the country is not absolute and is "subject to substantive limitations imposed by the Constitution." *Id.* at 620.

57. *Id.* at 618 n.13 (declining to decide what constitutes unreasonableness in border searches).

58. *See* Jared Janes, Article, *The Border Search Doctrine in the Digital Age: Implications of* Riley v. California *on Border Law Enforcement's Authority for Warrantless Searches of Electronic Devices*, 35 REV. LITIG. 71, 75-76 (2016) (noting not all border searches automatically reasonable).

59. *See* United States v. Cotterman, 709 F.3d 952, 963 (9th Cir. 2013) (en banc) (quoting United States v. Duncan, 693 F.2d 971, 977 (9th Cir. 1982)) (noting difficulty in defining clear dimensions of reasonable border search); *see also* Janes, *supra* note 58, at 76 (describing reluctance of Court to create clear boundaries of reasonableness).

60. *See Cotterman*, 709 F.3d at 963 (highlighting need for case-by-case analysis).

61. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 538, 541 & n.4 (1985) (distinguishing between routine and nonroutine searches at border); Rebecca M. Rowland, Note, *Border Searches of Electronic Devices*, 97 WASH. U. L. REV. 545, 547-48 (2019) (noting two types of border searches). The type of search conducted—routine versus nonroutine—determines the limits on what a border agent may search. *See* Rowland, *supra*, at 547-49 (distinguishing search methods available for routine and nonroutine searches).

62. United States v. Johnson, 991 F.2d 1287, 1291 (7th Cir. 1993); *see* Nowell, *supra* note 6, at 93 (contrasting routine and nonroutine searches at border).

and the balance of reasonableness is different "at the international border than in the interior."[63] Routine searches generally consist of less intrusive search methods, such as looking in luggage, bags, purses, or jackets, as well as pat down searches, the use of metal detectors or x-ray machines on luggage, and sniffing of a person by a narcotics dog.[64] In contrast, a search may be found nonroutine when it goes beyond a "limited intrusion" of the individual or their belongings.[65]

The Supreme Court briefly distinguished between "routine" and "nonroutine" border searches and seizures in *United States v. Montoya de Hernandez*.[66] There, the Court identified reasonable suspicion as the level of suspicion necessary to justify the detention of a traveler at the border "beyond the scope of a routine customs search and inspection."[67] Border officials detained the defendant, Montoya de Hernandez, whom they suspected was smuggling drugs into the United States in her alimentary canal.[68] Montoya de Hernandez was detained for sixteen hours before customs officials requested a court order authorizing a pregnancy test, an x-ray, and rectal examination.[69] The examination produced a balloon containing cocaine, of which she passed eighty-eight more over the next four days.[70]

---

63. *See Montoya de Hernandez*, 473 U.S. at 538 (defining routine searches at border).

64. *See* United States v. Lawson, 461 F.3d 697, 701-02 (6th Cir. 2006) (holding x-ray and drilling holes in luggage routine border search); United States v. Kelly, 302 F.3d 291, 294 (5th Cir. 2002) (holding sniffing by narcotics dog routine); United States v. Beras, 183 F.3d 22, 26 (1st Cir. 1999) (holding pat-down searches at border routine); *see also* Janes, *supra* note 58, at 76 (listing examples of routine searches at border). The court in *Kelly* articulated that when determining if a search is routine, "the key variable is the invasion of the privacy and dignity of the individual." *Kelly*, 302 F.3d at 294 (quoting United States v. Sandler, 644 F.2d 1163, 1167 (5th Cir. 1981)). Additionally, courts have defined intrusion in the context of a search not as physical invasion, but rather as the risk of "embarrassment, indignity, and invasion of privacy." United States v. Mejia, 720 F.2d 1378, 1382 (5th Cir. 1983).

65. *See* YULE KIM, CONG. RSCH. SERV., RL31826, PROTECTING OUR PERIMETER: BORDER SEARCHES UNDER THE FOURTH AMENDMENT 10 (2009), https://www.everycrsreport.com/files/20090629_RL31826_9ad182f9d94ca78136968036053b515bdd94dd40.pdf [https://perma.cc/6EBT-MD3G] (explaining when court may label search nonroutine).

66. 473 U.S. 531, 541 & n.4 (1985); *see* YULE KIM, CONG. RSCH. SERV., RL34404, BORDER SEARCHES OF LAPTOP COMPUTERS AND OTHER ELECTRONIC STORAGE DEVICES 2 (2009), https://fas.org/sgp/crs/homesec/RL34404.pdf [https://perma.cc/YWE2-KELB] (noting distinction in decision language).

67. *See Montoya de Hernandez*, 473 U.S. at 541 (setting forth holding). The Court noted that it had "not previously decided what level of suspicion would justify a seizure of an incoming traveler for purposes other than a routine border search." *Id.* at 540. In a footnote, the court explicitly noted that it was not deciding what level of suspicion is required for nonroutine border searches. *See id.* at 541 n.4.

68. *See id.* at 533-35 (describing customs officials' suspicions). The defendant, Montoya de Hernandez, raised suspicions when she arrived at the border in Los Angeles from Bogota, Colombia with $5,000 cash, no recollection of how her airline ticket was purchased, no checks or credit cards, and only a few changes of "cold weather" clothing. *See id.* at 533-34.

69. *See id.* at 535 (recounting length of detention and court order sought). During her detention, border agents gave Montoya de Hernandez the option of returning to Colombia on the next outgoing flight, consenting to an x-ray, or remaining detained until she had a monitored bowel movement. *See id.* at 534. She refused the x-ray, claiming to be pregnant, and instead chose to return to Colombia, but the officials were unable to place her on the next flight. *See id.* at 534-35.

70. *See id.* at 535-36 (detailing results of search).

The Court reiterated that routine searches at the border are per se reasonable, but that detentions that go beyond a routine search and inspection require reasonable suspicion.[71] The Court reasoned that, even though the detention "was beyond the scope of a routine customs search and inspection," it was "justified at its inception [because] customs agents, considering all the facts surrounding the traveler and her trip, reasonably suspect[ed] that the traveler [was] smuggling contraband in her alimentary canal."[72] In addition, the Court identified three examples of nonroutine searches, including strip searches, body-cavity searches, and involuntary x-ray searches, but explicitly stated that it was not holding what level of suspicion was required for nonroutine border searches.[73]

In *United States v. Flores-Montano*, the Court further relied on the distinction between routine and nonroutine searches to clarify the scope of the border search exception.[74] In *Flores-Montano*, customs officers stopped a car crossing into the United States at the California-Mexico border and, without reasonable suspicion, asked the driver to proceed to a secondary inspection site.[75] At the secondary inspection site, a mechanic removed the gas tank, and the customs officer subsequently discovered thirty-seven kilograms of marijuana.[76] The question as framed by the Court was whether the removal and dismantling of the fuel tank constituted a routine border search that did not require any level of suspicion.[77]

The Supreme Court reversed the Ninth Circuit's decision and held that the search of the gas tank did not require reasonable suspicion.[78] The Court declared that "[c]omplex balancing tests to determine what is a 'routine' search of a vehicle, as opposed to a more 'intrusive' search of a person, have no place in border searches of vehicles."[79] This decision implicitly limited the routine-nonroutine distinction to searches of persons rather than searches of property.[80] Further, the

71. *See id.* at 538, 541; Rowland, *supra* note 61, at 548 (noting suspicion standards for various types of searches and seizures).

72. United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985) (holding detention and search justified based on reasonable suspicion). The Court further explained that "not only is the expectation of privacy less at the border than in the interior, the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is also struck more favorably to the Government at the border." *Id.* at 539-40. In the majority opinion, Justice Rehnquist opined that while government interests at the border are high, customs agents must have reasonable suspicion, which the Court defined as a "particularized and objective basis for suspecting the particular person" of criminal activity. *Id.* at 541-42 (quoting United States v. Cortez, 449 U.S. 411, 417 (1981)).

73. *See id.* at 541 n.4 (1985) (providing examples of nonroutine searches). The Court footnoted what they *did not* hold in this case, and by doing so, provided examples of what constitutes a nonroutine search. *See id.*

74. *See* Alzahabi, *supra* note 39, at 168 (discussing continued focus on distinction between routine and nonroutine border searches).

75. *See* United States v. Flores-Montano, 541 U.S. 149, 150, 154 (2004) (outlining facts of case).

76. *See id.* at 151 (describing evidence uncovered after removal of gas tank). The total amount of time for this process was under an hour. *See id.* at 155 n.3.

77. *Id.* at 152 (presenting question).

78. *See id.* at 150 (explaining reversal of Ninth Circuit holding). The Ninth Circuit had previously held that the Fourth Amendment prohibited the search of the fuel tank absent reasonable suspicion. *Id.*

79. *See Flores-Montano*, 541 U.S. at 152 (differentiating between searches of vehicles and persons).

80. *See id.* (implying routine-nonroutine distinctions reserved for searches of persons).

Court left open the question of when, if ever, "a border search may be deemed 'unreasonable' because of the particularly offensive manner in which it was carried out."[81]

While these cases provide some guidelines, no clearly established test exists for determining what constitutes a routine search.[82] Establishing several facts, such as the degree of invasiveness or intrusiveness of the search, may assist in determining whether a search is routine.[83] For example, a search is more likely to be considered nonroutine when it is objectively intrusive, such as causing significant property damage or embarrassing the individual.[84] The First Circuit developed a non-exhaustive list of factors to assist in this determination, including: whether the search resulted in exposure of any intimate body parts or required the suspect to remove clothing, whether the customs officer made physical contact with the suspect during the search, whether force was used, whether the type of search subjected the suspect to pain or danger, the "overall manner in which the search was conducted," and "whether the suspect's reasonable expectations of privacy, if any, were abrogated by the search."[85] The Supreme Court, however, has not determined the level of suspicion required to justify conducting a nonroutine search, but the widely accepted standard is reasonable suspicion.[86]

3. Searches of Electronic Devices at the Border

Each year, millions of people travel in and out of the United States with electronic devices.[87] On a typical day in 2018, CBP processed 1,133,914 passengers

81. United States v. Flores-Montano, 541 U.S. 149, 154 n.2 (2004) (quoting United States v. Ramsey, 431 U.S. 606, 618 n.13 (1977)).

82. *See* KIM, *supra* note 65, at 10 (noting lack of clear rule for determining routine or nonroutine search).

83. *See id.* (suggesting facts to consider).

84. *See* United States v. Kelly, 302 F.3d 291, 294 (5th Cir. 2002) (describing invasion of privacy and potential for embarrassment resulting from nonroutine searches); KIM, *supra* note 65, at 1, 10 (discussing distinguishing characteristics of nonroutine searches).

85. United States v. Braks, 842 F.2d 509, 512 (1st Cir. 1988); *see* KIM, *supra* note 65, at 10 (listing factors suggested by First Circuit); Janes, *supra* note 58, at 76-77 (describing importance of context in factors suggested by First Circuit). The court compiled this list by looking at factors highlighted by the Supreme Court and several federal appellate courts to determine "the degree of invasiveness that accompanies any particular search." *See Braks*, 842 F.2d at 512.

86. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985) (noting reasonable suspicion standard applies in various contexts); Ahad Khilji, Comment, *Warrantless Searches of Electronic Devices at U.S. Borders: Securing the Nation or Violating Digital Liberty?*, 27 CATH. U. J.L. & TECH., Spring 2019, at 185 (noting absence of articulated level of suspicion required for nonroutine searches); *see also supra* note 37 and accompanying text (defining probable cause and reasonable suspicion outside border search context).

87. *See* CBP FY17 Statistics, *supra* note 5 (stating CBP processed almost 400 million international travelers in fiscal year 2017); PORTABLE ELEC. DEVICES AVIATION RULEMAKING COMM., RECOMMENDATIONS ON EXPANDING THE USE OF PORTABLE ELECTRONIC DEVICES DURING FLIGHT app. H-8 (2013), https://www.faa.gov/about/initiatives/ped/media/PED_ARC_FINAL_REPORT.pdf [https://perma.cc/GK43-PA7Z] (noting 94% of adult U.S. airline passengers traveled with at least one electronic device).

and pedestrians at the border.[88] It is likely most of these individuals traveled with an electronic device that could have been searched by CBP absent a warrant or suspicion.[89] Additionally, the number of searches of electronic devices is growing.[90] CBP searched more electronic devices in the first four months of 2017 than in all of 2015, and over 10,000 more throughout 2017 as compared to 2016.[91]

a. Manual Versus Forensic Searches of Electronic Devices at the Border

Electronic searches at the border take two forms, manual and forensic.[92] Manual searches involve the most basic technique of gathering information from a device and allow access solely to information available by "point-and-click" operations.[93] Manual searches use only the inputs built in to the device and do not require any specialized tools.[94] While manual searches involve a basic scroll though calls and texts on a smart phone or looking through files saved locally on a computer, the amount of digital information examined can still be extensive.[95]

---

88. *See* U.S. CUSTOMS & BORDER PATROL, DEP'T OF HOMELAND SEC., ON A TYPICAL DAY IN FISCAL YEAR 2018, CBP . . . , https://www.cbp.gov/newsroom/stats/typical-day-fy2018 [https://perma.cc/R4JK-YUF3] (last modified Mar. 7, 2019) (noting daily statistics for 2018).

89. *See supra* note 87 and accompanying text (citing CBP statistics and statistics concerning number of travelers carrying electronic devices); O'Grady, *supra* note 12, at 2258-59 (summarizing CBP search statistics). All entrants to the United States—visitors, permanent residents, and U.S. citizens—are all subject to CBP search of their electronic devices. *See* Khilji, *supra* note 86, at 176 (cautioning even U.S. citizens subject to warrantless search of electronic devices).

90. *See* CBP FY17 Statistics, *supra* note 5 (reporting increase in electronic searches at border from 2016 to 2017).

91. *See id.* (providing amount of electronic searches in first four months of 2017 in excess of 9,000); Press Release, Dep't of Homeland Sec., U.S. Customs & Border Prot., CBP Releases Statistics on Electronic Device Searches (Apr. 11, 2017), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0 [https://perma.cc/URW4-B6MB] (noting 8,503 total electronic searches in 2015); *see also* Tim Cushing, *Phone Searches Now Default Mode at the Border; More Searches Last Month than in All of 2015*, TECHDIRT (Mar. 14, 2017, 10:49 AM), https://www.techdirt.com/articles/20170314/08063936914/phone-searches-now-default-mode-border-more-searches-last-month-than-all-2015.shtml [https://perma.cc/DXV3-QLV9] (discussing significant increase in border searches of electronic devices). While CBP reports searching less than 0.1% of all travelers' electronic devices in 2017, this amount nearly doubled from 2016. *See* CBP FY17 Statistics, *supra* note 5.

92. *See* De Leon, *supra* note 11, at 555 (explaining two types of digital searches); Miller, *supra* note 24, at 1963-64 (noting different forms of digital searches at border). Manual searches are otherwise known as "basic" or "routine," and forensic searches are also called "nonroutine" or "advanced." De Leon, *supra* note 11, at 555 n.8; Directive No. 3340-049A from U.S. Customs & Border Prot. on Border Search of Electronic Devices 5-6 (Jan. 4, 2018), https://www.dhs.gov/sites/default/files/publications/CBP%20Directive%203340-049A_Border-Search-of-Electronic-Media.pdf [https://perma.cc/JC25-HU2Z] [hereinafter CBP Directive].

93. *See* Nowell, *supra* note 6, at 93 (detailing manual search); SEAN E. GOODISON ET AL., RAND CORP., DIGITAL EVIDENCE AND THE U.S. CRIMINAL JUSTICE SYSTEM 5 (2015), https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf [https://perma.cc/5T6P-EED3] (providing detailed description of manual search technique).

94. *See* GOODISON ET AL., *supra* note 93, at 5 (explaining manual techniques). Manual searches allow access to information contained locally on the phone and do not provide access to deleted material. *See id.*

95. *See* United States v. Kolsuz, 890 F.3d 133, 139 (4th Cir. 2018) (describing scrolling function of manual search); Miller, *supra* note 24, at 1963 (explaining potential for extensive examination).

Both the amount of time an officer has to search a device and the officer's knowledge of that device's operating system can have a significant impact on the amount of personal data examined in a manual search.[96] Further, the information obtained by a manual search can reveal sensitive and private information about the individual.[97]

Forensic searches, on the other hand, require the use of tools or software to access data on an electronic device.[98] Several factors distinguish these more advanced searches: officers conduct them away from the border, officers confiscate the device, the search allows full access to and duplication of hard drives, and they generally take more time.[99] The distinction between manual and forensic searches is not always clear, but courts generally look to the method of the search as opposed to the information gathered.[100] For example, in *United States v. Saboonchi*,[101] the court identified three capabilities unique to forensic searches: creation of a copy of the hard drive, access to deleted information, and information gathering about the individual's activities away from the border.[102]

b. Current CBP Policy

In January 2018, CBP released a directive that updated its official policy on procedures regarding searches of electronic devices at the border.[103] The policy asserts that border searches of electronic devices are "essential to enforcing the law at the U.S. border and to protecting border security."[104] The policy

96. *See* Miller, *supra* note 24, at 1963 (noting significant impact of length permitted for search); GOODISON ET AL., *supra* note 93, at 5 (explaining impact of knowledge on manual searches).

97. *See* Khilji, *supra* note 86, at 187 (outlining broad range of personal information potentially obtained by manual search). In a manual search, agents can access text messages, contacts, phone calls, photos, videos, e-mails, and browsing history, as well as more sensitive information such as an individual's religious or political beliefs, sex life, and finances. *See id.*

98. *See* Nowell, *supra* note 6, at 93 (describing more exhaustive methods of forensic search).

99. *See* De Leon, *supra* note 11, at 555 (describing characteristics of forensic search); Miller, *supra* note 24, at 1964 (comparing manual and forensic searches).

100. *See* Khilji, *supra* note 86, at 187 (noting "blurred" distinction between manual and forensic searches); *see also* Miller, *supra* note 24, at 1964 (explaining difficulty distinguishing between manual and forensic searches).

101. 990 F. Supp. 2d 536 (D. Md. 2014).

102. *See id.* at 564 (articulating distinct concerns regarding forensic searches); *see also* Miller, *supra* note 24, at 1964-65 (providing example of distinctions made by *Saboonchi* court).

103. *See* CBP Directive, *supra* note 92, at 1; U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT UPDATE FOR CBP BORDER SEARCHES OF ELECTRONIC DEVICES DHS/CBP/PIA-008(a), at 1 (Jan. 4, 2018), https://www.dhs.gov/sites/default/files/publications/PIA-CBP%20-%20Border-Searches-of-Electronic-Devices%20-January-2018%20-%20Compliant.pdf [https://perma.cc/4S47-7HLB] [hereinafter DHS ASSESSMENT] (detailing CBP Privacy Impact Assessment).

104. CBP Directive, *supra* note 92, at 1 (stating purpose of directive). The directive lists the following ways in which these searches help prevent contraband smuggling and other crime:

> They help detect evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband and child pornography. [R]eveal information about financial and commercial crimes . . . They can be vital to risk assessments . . . and they can enhance critical information

distinguishes between manual and forensic searches and limits a search based on its type.[105]

Under the policy, a manual search is defined as anything that is not a forensic search.[106] During a manual search, an officer "may examine an electronic device and may review and analyze information encountered at the border" with or without suspicion.[107] Nevertheless, an officer is prohibited from accessing information stored remotely and must ensure that the phone or device is in "airplane" mode before performing a manual search.[108]

In contrast, an "advanced" or forensic search is where an officer "connects external equipment . . . to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents."[109] To conduct a forensic search, an officer must have either reasonable suspicion of criminal activity or a national security concern.[110] While the policy does not allow for full discretion, it grants customs officials broad authority to conduct warrantless and suspicionless searches of electronic devices, which some scholars and legal commentators consider unconstitutional.[111]

> sharing with, and feedback from, elements of the federal government responsible for analyzing terrorist threat information. Finally, searches . . . are often integral to a determination of an individual's intentions upon entry and provide additional information relevant to admissibility under immigration laws.

Id.

105. *See* CBP Directive, *supra* note 92, at 4-5 (defining two types of electronic searches at border); Bohannon, *supra* note 29, at 575 (noting CBP policy distinguishes between basic and advanced searches). CBP uses the terminology "basic" for a manual search and "advanced" for a forensic search. *See* CBP Directive, *supra* note 92, at 4-5. CBP refers to the two types of searches as "basic" and "advanced" searches; for clarity, this Note uses the terms manual and forensic. *See id.*

106. *See* CBP Directive, *supra* note 95, at 4-5 (defining basic and manual search).

107. *Id.* at 4 (declaring no suspicion required for manual search of electronic device). In support of a lack of suspicion requirement for manual searches, the policy references case law and statutes that support the notion that border searches are "not subject to any requirement of reasonable suspicion, probable cause, or warrant." *See id.* at 3 (quoting United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985)).

108. *See id.* at 4 (mandating connectivity to any network disabled before search). The policy states that the officer will either request that the individual turn off the connectivity, or "where warranted by national security," the officer will disable the connection. *See id.* In the case of a password-protected device, the officer may request the password from the individual, and if the officer is unable to inspect the device because of the password, the officer may detain the device. *See id.* at 6.

109. *Id.* at 5 (defining advanced search).

110. *See* CBP Directive, *supra* note 95, at 5 (stating requirements to perform advanced search). The Directive states that "many factors may create reasonable suspicion or constitute a national security concern." *Id.* Some opponents of the policy view the national security clause as a loophole that allows officers greater discretion to perform advanced searches. *See* Khilji, *supra* note 86, at 187 (articulating concerns with updated CBP policy).

111. *See* Carroll, *supra* note 50, at 8 (describing authority set out in policy unconstitutional); Khilij, *supra* note 86, at 187 (criticizing CBP's broad discretion to initiate forensic search).

C. The Fourth Amendment and Digital Privacy

The Supreme Court has opined on the warrant requirement for searching electronic devices in two specific contexts: search incident to arrest and cell-site records.[112]

1. Search Incident to Arrest: Riley v. California

In the landmark case, *Riley v. California*, the Court limited the search incident to arrest exception to the warrant requirement, greatly influencing the treatment of electronic device searches under the Fourth Amendment.[113] In *Riley*, the Court consolidated two cases involving the warrantless search and seizure of a cell phone incident to a lawful arrest.[114] The common question presented to the Court was "whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested."[115] The search incident to arrest exception has been historically justified by the heightened government interests in protecting its officers and preserving evidence.[116] The Court, however, held that these policy reasons are not present when the search of a cell phone involves digital data, as opposed to physical contraband, and that officers must "generally secure a warrant before conducting a search."[117]

The Court rejected the government's argument that the data stored on a cell phone is "materially indistinguishable" from searches of other physical items, analogizing this argument to the statement "a ride on horseback is materially indistinguishable from a flight to the moon."[118] The Court articulated that the

112. *See* DeSimone, *supra* note 25, at 713 (noting two contexts Court considered warrant requirement).

113. *See* Riley v. California, 573 U.S. 373, 386 (2014) (holding warrant required for search of electronic device incident to arrest); Rowland, *supra* note 61, at 549 (noting impact of *Riley* on Fourth Amendment application to electronic devices).

114. *See Riley*, 573 U.S. at 378 (noting consolidation of two cases); Bohannon, *supra* note 29, at 568 (calling two cases companion cases).

115. *Riley*, 573 U.S. at 378.

116. *See* Chimel v. California, 395 U.S. 752, 762-63 (1969) (providing main purpose of search incident to lawful arrest exception); *see also Riley*, 573 U.S. at 383 (citing *Chimel* arrest exception); Rowland, *supra* note 61, at 550 (describing policy reasons for exception). The safety of the officer is in jeopardy if the arrestee has a weapon that can be used to resist arrest or aid in escaping. *Chimel*, 395 U.S. at 762-63 (outlining main safety concerns for officers). Additionally, the officer can "search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction." *Id.* at 763. The items searched are limited to "personal property . . . immediately associated with the person of the arrestee." United States v. Chadwick, 433 U.S. 1, 15 (1977).

117. *See Riley*, 573 U.S. at 386 (holding *Chimel* factors not present in digital search of cell phone and warrant required). An officer is still free to search a device for weapons or contraband, such as a hidden razor blade that might be used to harm the arresting officer. *See id.* at 387. The Court reasoned that data on a cell phone cannot be used as a weapon to harm an arresting officer. *Id.* Additionally, while the Court acknowledged that there may be some concern that the arrestee will remotely wipe data from the phone to destroy evidence, it did not hold that the risk could only be avoided by a warrantless search of digital data. *See id.* at 388-90. The Court suggested other ways to prevent this risk, such as turning off the phone, removing its battery, disconnecting the phone from the network, or putting it in an enclosure that prevents any connection or signal. *See id.* at 390.

118. *Id.* at 393 (reasoning little justification for government's characterization).

privacy concerns implicated in searching the digital content of a cell phone are categorically different from other searches of personal property during an arrest in both "a quantitative and a qualitative sense."[119] The quantity of information stored on a cell phone is vastly different than the papers or pictures a person can put in their pocket or wallet, and allows people to carry "a cache of sensitive personal information with them as they [go] about their day."[120] The quality of information stored digitally is also vastly different and can contain information about an individual's medical diagnosis, financial status, religious and political affiliation, as well as sexual associations.[121] The Court drew a hard line by holding that law enforcement must obtain a warrant before accessing an individual's digital data during a search incident to arrest, and courts have attempted to extend this logic to other Fourth Amendment disputes, including the border search exception.[122]

2. Cell-Site Records: Carpenter v. United States

Four years after *Riley*, the Court continued its discussion of digital data searches in the context of cell-site records in *Carpenter v. United States*.[123] The question before the Court in *Carpenter* was whether the government could conduct a warrantless search of cell-site records to track an individual's location and movements.[124] The government argued the warrantless search was valid under the third-party doctrine, which states that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[125] The lower courts agreed with the government and held that Carpenter had no reasonable

119. *See* Riley v. California, 573 U.S. 373, 393 (2014) (emphasizing difference between digital data and other personal property).

120. *See id.* at 393-95 (detailing quantitative differences). The Court noted that nearly 90% of Americans who own smartphones use them to store records of "nearly every aspect of their lives—from the mundane to the intimate." *Id.* at 395. Cell phones have large storage capacity and can contain years of personal information including photographs, messages, calendars, browsing history, and location and GPS data. *See id.* at 394, 396.

121. *See id.* at 395-96 (describing qualitative differences). The Court also cautioned that once border agents access a cell phone, it is easy to access information stored in the cloud, which creates additional privacy concerns. *See id.* at 397. "Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself." *Id.*

122. *See id.* at 403 (holding warrant required); DeSimone, *supra* note 25, at 709 (analyzing *Riley* holding); O'Grady, *supra* note 12, at 2271 (describing *Riley*'s significant impact on electronic border search debate).

123. 138 S. Ct. 2206 (2018); *see* DeSimone, *supra* note 25, at 709 (noting context and timing of case); Rowland, *supra* note 61, at 551 (describing continued discussion by Court).

124. *See Carpenter*, 138 S. Ct. at 2214-15 (presenting novel question before Court). "The question we confront today is how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals." *Id.* at 2216.

125. *Id.* (quoting Smith v. Maryland, 442 U.S. 735, 743-44 (1979)) (stating basis of government's argument). Under the third-party doctrine, "the Government is typically free to obtain such information from the recipient without triggering Fourth Amendment protections." *Id.*

expectation of privacy because he voluntarily shared his location information with his wireless carrier.[126]

The Court reversed the decision, holding that while cell-site records are discoverable, law enforcement cannot obtain them without a warrant supported by probable cause.[127] The Court distinguished cell-site records from other business records by highlighting how cell-site records provide information that is "detailed, encyclopedic, and effortlessly compiled."[128] Such information provides the government with an "intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[129] *Carpenter* echoed the tone in *Riley*, distinguishing digital data from other personal effects and presenting a strong case for prohibiting warrantless searches of electronic devices in other contexts.[130] While neither case addressed electronic searches at the border, they set the stage for arguments against warrantless searches of electronics under the border search exception.[131]

D. Applicability of Riley *to Border Searches: Circuit Split*

The Supreme Court has yet to address whether the border search exception includes warrantless searches of electronic devices.[132] The lack of clarification by the Court has resulted in the existing circuit split regarding whether *Riley*'s warrant requirement for cell phone searches extends to forensic searches of electronic devices at the border.[133] The Ninth and Fourth Circuits require some level of reasonable suspicion for forensic searches of electronic devices, while the

126. *Id.* at 2213 (citing decision of lower court). The Court of Appeals for the Sixth Circuit held, "Given that cell phone users voluntarily convey cell-site data to their carriers . . . the resulting business records are not entitled to Fourth Amendment protection." *Id.*

127. *See id.* at 2221 (holding warrant required for cell-site records). The Court clarified that its holding was narrow and did not apply to all business records, surveillance techniques, or tools. *See id.* at 2220. Unlike business records, such as bank records or call records, a person does not voluntarily share their location when their cell phone location data is gathered. *See id.* This information is shared simply by turning on one's phone and does not involve any meaningful affirmative consent by the phone's user. *See id.*

128. *Carpenter*, 138 S. Ct. at 2216 (comparing unique nature of cell-site records to GPS data).

129. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)) (reiterating unique nature of information gathered from cell-site records).

130. *See* Rowland, *supra* note 61, at 552 (noting significance of *Riley* and *Carpenter* to Fourth Amendment doctrine).

131. *See* Das, *supra* note 45, at 232 (discussing application of rationales in *Riley* and *Carpenter* to other cases); O'Grady, *supra* note 12, at 2273 (articulating different application by lower courts of *Riley* and *Carpenter* to electronic border searches).

132. *See* United States v. Molina-Isidoro, 884 F.3d 287, 292 (5th Cir. 2018) (noting no Supreme Court decision addressing electronic border searches); DeSimone, *supra* note 25, at 713 (acknowledging lack of decision from Court); Nowell, *supra* note 6, at 95 (stating Court yet to address electronic searches in border search context).

133. *See* De Leon, *supra* note 11, at 555 (outlining circuit split regarding forensic searches of electronic devices); Rowland, *supra* note 61, at 546 (describing issue of contradiction between courts); *supra* note 122 (providing *Riley*'s holding).

Eleventh Circuit does not require any level of suspicion for digital searches at the border.[134] Even though the circuits are split on the level of suspicion required, no court has held that probable cause or a warrant are required to conduct an electronic search at the border.[135]

1. Ninth Circuit: United States v. Cotterman*: Reasonable Suspicion Required for Forensic Searches*

United States v. Cotterman preceded *Riley*, but it raised similar privacy concerns about the encyclopedic and sensitive nature of information stored on cell phones.[136] In *Cotterman*, during a primary inspection at the Mexico-United States border, the Treasury Enforcement Communication System (TECS) alerted CBP agents that Cotterman was a convicted sex offender who was potentially involved in child sex tourism.[137] Based on the TECS information, the agents directed Cotterman and his wife to a secondary inspection location, where agents searched the vehicle and found two laptops and three cameras.[138] An initial search did not reveal any criminal material, but due to the existence of multiple password-protected files, agents seized the laptops and cameras and took them over 170 miles away for a forensic examination, which uncovered child pornography.[139] After a grand jury indicted him, Cotterman moved to suppress the evidence discovered on his laptop.[140] The district court granted his motion, but the Ninth Circuit reversed on an interlocutory appeal, then upheld the reversal on a rehearing en banc.[141]

In *Cotterman*, the court considered what level of suspicion is required for a warrantless forensic search of an electronic device: no suspicion, reasonable suspicion, or probable cause.[142] In its decision, the court held that agents must have reasonable suspicion of criminal activity before conducting a forensic search of an electronic device.[143] The Ninth Circuit reasoned that a laptop

134. *See* United States v. Touset, 890 F.3d 1227, 1229 (11th Cir. 2018) (holding no suspicion required); United States v. Kolsuz, 890 F.3d 133, 144 (4th Cir. 2018) (holding individualized suspicion required); United States v. Cotterman, 709 F.3d 952, 968 (9th Cir. 2013) (en banc) (holding reasonable suspicion required for forensic search).

135. *See* Nowell, *supra* note 6, at 96 (highlighting lack of rulings in favor of requiring probable cause or warrant).

136. *See Cotterman*, 709 F.3d at 965 (observing large amount of highly sensitive and personal data stored on electronic devices); Rowland, *supra* note 61, at 555 (noting similar concerns addressed in *Cotterman*).

137. *See Cotterman*, 709 F.3d at 957 (noting details of TECS information).

138. *See id.* (recounting items found in secondary site search).

139. *See id.* at 958 (detailing forensic examination of laptops and camera). Immigration and Customs Enforcement (ICE) agents copied the laptop hard drives and found child pornography. *See id.*

140. *See* United States v. Cotterman, 709 F.3d 952, 959 (9th Cir. 2013) (en banc) (recognizing district court decision).

141. *See id.* at 959, 970 (summarizing procedural history and holding at Ninth Circuit).

142. *See id.* at 959-60 (stating question before court).

143. *See id.* at 968 (holding forensic examination of laptop required reasonable suspicion). The Ninth Circuit reversed the grant of the motion to suppress the results of the laptop search, holding that the border agents had reasonable suspicion to conduct the forensic searches. *See id.* at 970.

contains "uniquely sensitive" data and analogized a forensic search of a hard drive to that of a strip search.[144] Additionally, the court distinguished between manual searches and forensic searches, stating that forensic searches are "akin to reading a diary line by line looking for mention of criminal activity—plus looking at everything else the writer may have erased."[145] Notably, the court allowed manual searches of electronic devices without any suspicion.[146]

2. *Fourth Circuit:* United States v. Kolsuz*: Reasonable Suspicion Required for Forensic Searches*

In *United States v. Kolsuz*, the Fourth Circuit mirrored the stance taken by the Ninth Circuit and followed the reasoning set forth in *Riley*, holding that a forensic search of an electronic device requires some level of individualized suspicion.[147] While attempting to board a flight to Turkey from the United States, the defendant, Hamza Kolsuz, was detained by customs officers after firearm parts were discovered in his luggage during a routine inspection.[148] Customs officers then conducted a manual search of his phone, scrolling through recent calls and text messages, before sending the phone off site for a forensic examination.[149] The forensic examination took one month to complete and yielded a nearly 900-page report.[150] The district court upheld the search, finding it was supported by reasonable suspicion.[151]

On appeal, Kolsuz argued that, under *Riley*, the government must have more than reasonable suspicion to conduct a forensic search of an electronic device, and that a warrant supported by probable cause is required.[152] The Fourth Circuit affirmed the judgment of the district court to admit evidence obtained from the search.[153] The court agreed with the district court, as well as the Ninth Circuit in *Cotterman*, that a forensic search requires some level of individualized suspicion, but declined to resolve the question of precisely what that standard should be.[154]

---

144. *See Cotterman*, 709 F.3d at 966 (describing intrusiveness of forensic search).

145. *Id.* at 962-63 (characterizing forensic searches invasive).

146. *See* United States v. Cotterman, 709 F.3d 952, 960-61, 967 (9th Cir. 2013) (en banc) (noting agents may still conduct manual searches of electronics without suspicion).

147. *See* United States v. Kolsuz, 890 F.3d 133, 137, 144 (4th Cir. 2018) (holding forensic search requires some form of individualized suspicion).

148. *See id.* at 136 (recounting underlying case facts).

149. *See id.* at 139 (detailing two separate phone searches).

150. *See id.* (describing lengthy report obtained from forensic search). The entire forensic search was completed while the phone was in airplane mode, demonstrating how much data can be obtained even when a device is not connected to a network. *See id.*

151. *See Kolsuz*, 890 F.3d at 137 (providing overview of district court's decision).

152. *See id.* (outlining Kolsuz's argument on appeal). Kolsuz alternatively argued that once the government removed the phone from the airport, the subsequent forensic analysis no longer constituted a border search. *See id.* at 136-37. The court categorically rejected this argument and held that "[d]espite the temporal and spatial distance" between the site and the airport, the "justification for the border search is broad enough to reach the search." *Id.* at 137.

153. *See* United States v. Kolsuz, 890 F.3d 133, 137 (4th Cir. 2018) (affirming district court's judgment).

154. *See id.* at 137, 144-46 (supporting decision).

Additionally, the court pointedly separated manual and forensic searches, explicitly categorizing forensic searches as nonroutine, but nevertheless upheld the forensic search.[155]

3. Eleventh Circuit: United States v. Touset*: No Suspicion Required for Digital Searches at the Border*

Two weeks after the Fourth Circuit's decision in *Kolsuz*, the Eleventh Circuit weighed in on the application of the border search exception to searches of electronic devices in *United States v. Touset*, and unequivocally rejected the holdings in *Cotterman* and *Kolsuz*.[156] In *Touset*, border agents stopped the defendant, Karl Touset, upon arrival in the United States, based on a "look-out" placed on Touset by the Department of Homeland Security for suspicion of involvement with child pornography.[157] After stopping Touset, agents proceeded to inspect his luggage and found two iPhones, a camera, two laptops, two external hard drives, and two tablets.[158] Agents manually searched the iPhones and the camera before returning them to Touset, but detained the remaining devices for forensic analysis, which revealed child pornography on multiple devices.[159]

The district court denied Touset's motion to suppress the evidence obtained in the search.[160] On appeal, the court considered whether a forensic search of an electronic device at the border requires reasonable suspicion under the Fourth Amendment.[161] Following its recent decision in *United States v. Vergara*,[162] the Eleventh Circuit held that forensic searches of electronic devices *never* require individualized suspicion and that *Riley* does not apply at the border.[163] The *Touset* court emphasized the distinction between searches of property and searches of people stating, "[t]he Supreme Court has never required reasonable suspicion for a search of property at the border, however non-routine and intrusive, and neither have we."[164] The Eleventh Circuit additionally noted that it was

155. *See id.* at 137, 147 (categorizing forensic searches nonroutine and upholding search). The Fourth Circuit agreed with the district court in that "a forensic border search of a phone must be treated as nonroutine, permissible only on a showing of individualized suspicion." *Id.* at 144. The court grouped forensic searches with previously identified nonroutine searches such as "strip searches, alimentary-canal searches, x-rays, and the like." *Id.*

156. *See* United States v. Touset, 890 F.3d 1227, 1234 (11th Cir. 2018) (rejecting Ninth and Fourth Circuit approaches). In its decision, the court detailed the holdings in the two cases and flatly stated, "We are unpersuaded." *Id.*

157. *See id.* at 1230 (outlining case facts).

158. *Id.* (listing electronic devices found during inspection).

159. *Id.* The iPhones and camera were returned to Touset after the manual search did not uncover any child pornography. *See id.*

160. *See Touset*, 890 F.3d at 1231 (noting opinion of district court and subsequent appeal).

161. *See id.* at 1229 (stating question before court).

162. 884 F.3d 1309 (11th Cir. 2018).

163. *See* United States v. Touset, 890 F.3d 1227, 1229, 1234 (11th Cir. 2018) (holding neither reasonable suspicion nor *Riley* exception required for border search).

164. *Id.* at 1233 (stressing distinction between searches of property and people). The court detailed times when the Supreme Court held that a search was nonroutine and emphasized that those decisions dealt with

unwilling to "create a special rule that will benefit offenders who now conceal contraband in a new kind of property," and that the responsibility of border agents to prevent contraband from entering the United States has not changed just because technology has.[165]

E. International Students and Higher Education in the United States

1. The Numbers: A Decline in New International Student Enrollment

During the 2018-2019 academic year, 1,095,299 international students were enrolled in U.S. colleges and universities.[166] The United States is the top destination for international students, hosting nearly one-quarter of the 4.6 million students enrolled worldwide.[167] While the overall number of students increased in from the previous academic year, new student enrollment fell by almost 7%, in accordance with the ongoing decline that started in the 2015-2016 academic year.[168] In the 2017-2018 academic year, enrollment decreased primarily at the graduate and non-degree levels.[169] In the 2018-2019 academic year, however, the decrease in enrollment was primarily at the undergraduate level.[170]

The decrease in international student enrollment will likely have a negative impact on the financial stability and campus diversity of colleges and universities.[171] International students have significant impact on the U.S. economy, contributing $38.7 billion and supporting more than 415,000 jobs during the 2019-

searches of people, not property. *See id.* The panel further noted that its own precedent shows an unwillingness "to distinguish between different kinds of property." *See id.*

165. *Id.* at 1233, 1236 (emphasizing reasons border search exception must apply to electronic devices).

166. *See* Press Release, Inst. of Int'l Educ., Number of International Students in the United States Hits All-Time High (Nov. 18, 2019), https://www.iie.org/Why-IIE/Announcements/2019/11/Number-of-International-Students-in-the-United-States-Hits-All-Time-High [https://perma.cc/93K3-FYQR] (announcing number of international students); INST. OF INT'L EDUC., *supra* note 7, at 19 (citing detailed enrollment data and showing increase). Data shows that the number of international students enrolled in colleges and universities in the United States surpassed one million for four consecutive years, making up 5.5% of the total higher education population in the United States. *See* Press Release, Inst. of Int'l Educ., *supra*.

167. *See* Jie Zong & Jeanne Batalova, *International Students in the United States*, MIGRATION POL'Y INST. (May 9, 2018), https://www.migrationpolicy.org/article/international-students-united-states [https://perma.cc/YY2W-PFY8] (noting large percentage of international students choose to study in United States).

168. *See* Press Release, Inst. of Int'l Educ., Number of International Students in the United States Reaches New High of 1.09 Million (Nov. 13, 2018), https://www.iie.org/Why-IIE/Announcements/2018/11/2018-11-13-Number-of-International-Students-Reaches-New-High [https://perma.cc/9PLZ-AZRC] (cautioning increase in numbers does not tell full story); *see also* INST. OF INT'L EDUC., *supra* note 7, at 19 (quantifying decrease in new student enrollment).

169. *See* Press Release, Inst. of Int'l Educ., *supra* note 168 (clarifying 2017-2018 decrease primarily at graduate level).

170. *See* INST. OF INT'L EDUC., *supra* note 7, at 19 (contrasting 2.4% enrollment decrease at undergraduate level up from 0.8% in previous year).

171. *See* Wong, *supra* note 18 (describing concerns of U.S. colleges and universities). William Stock, an immigration lawyer working with universities, argued the administration's policies that deter "international students from attending U.S. colleges . . . is hindering schools' ability to build diverse student bodies—and depleting their budgets." *Id.*

2020 academic year.[172] Notably, most international students received their funding from outside the United States.[173] Because of this, international students contribute disproportionately to tuition, with one study estimating that international students account for more than one-quarter of tuition revenue at public universities.[174] Some universities have prepared for the potential for negative financial impact by taking out insurance policies to protect the schools in case of a significant drop in international enrollment.[175]

2. Cause of the Decline

Among the possible reasons for the decline in new international student enrollment are "visa application issues or delays/denials, the increasingly competitive global market of higher education options, the social and political environment, and the costs of U.S. higher education."[176] Schools overwhelmingly cite visa application issues and delays or denials as the top reason for the decline in new enrollment, with global competition and the social and political environment as other leading causes.[177] The visa obstacles, at least in part, trace back to President Donald Trump's 2017 memorandum that called for "'heightened screening and vetting of applications for visas and other immigration benefits,' as well as new or updated requirements for visa holders studying or working at U.S. colleges."[178]

---

172. *See* NAFSA, *supra* note 8 (citing statistics regarding financial impact of international students); Press Release, Inst. of Int'l Educ., *supra* note 168 (discussing financial impact of international students). International students contribute financially to U.S. universities through tuition, room and board, and other expenses. *See* Press Release, Inst. of Int'l Educ., *supra* note 168.

173. *See* Zong & Batalova, *supra* note 167 (stating various sources of funding for international students). In the 2016-2017 academic year, "60 percent relied on personal and family funding . . . 6 percent . . . used foreign government or university aid. The remaining 34 percent financed their education primarily through current employment, U.S. university or government aid, or other sources." *Id.*

174. Nathan Grawe, *International Students and U.S. Higher Education*, ECONOFACT (July 17, 2019), https://econofact.org/international-students-and-u-s-higher-education [https://perma.cc/L2J4-4SWJ] (describing major financial impact of international students).

175. *See* Jillian Berman, *Why Are International Students Turning Their Back on American Colleges?*, MARKETWATCH (Feb. 7, 2019, 9:34 AM), https://www.marketwatch.com/story/the-number-of-international-students-coming-to-the-us-for-grad-school-declined-for-the-second-year-in-a-row-2019-02-07 [https://perma.cc/9F7X-SSKQ] (reporting precautionary step taken by University of Illinois's engineering and business schools).

176. JODI SANGER & JULIE BAER, INST. OF INT'L EDUC., FALL 2019 INTERNATIONAL STUDENT ENROLLMENT SNAPSHOT SURVEY 5 (2019), https://www.iie.org/Research-and-Insights/Publications/Fall-2019-International-Student-Enrollment-Survey [https://perma.cc/AX9B-S37P]; Berman, *supra* note 175 (describing possible reasons for decline); Zong & Batalova, *supra* note 167 (listing multiple factors contributing to decline).

177. *See* Berman, *supra* note 175 (noting political rhetoric one main factor); SANGER & BAER, *supra* note 176, at 6 (reporting results of survey); Wong, *supra* note 18 (citing delay or denial of student visas contributing factor). In the Institute of International Education's 2018-2019 survey, 86.9% of institutions that participated cited visa application process issues, delays, or denials as the top contributing factor to drops in enrollment, an increase from 68.4% in fall 2017. SANGER & BAER, *supra* note 176, at 6.

178. Wong, *supra* note 18 (quoting Implementing Immediate Heightened Scrutiny and Vetting of Applications for Visas, 82 Fed. Reg. 16,279 (Mar. 6, 2017)) (setting forth NAFSA findings concerning effect of political action).

3. Impact of Electronic Searches at the Border

The threat of one's visa being revoked at the border based on a potential suspicionless search of his or her electronic devices compounds the uncertainty and stress regarding the visa process and potential delays and denials.[179] At least two incidents occurred at the beginning of the 2019-2020 academic year in which international students' visas were revoked after customs officers searched their electronic devices.[180] In the case of Ismail Ajjawi, the incoming Harvard College student, CBP denied entry after officers searched his phone and found posts by Ajjawi's friends on social media deemed by the officers to be anti-American.[181] According to Ajjawi, there is no indication that CBP officers found posts by Ajjawi expressing any political views.[182]

The same month CBP revoked Ajjawi's visa and sent him back to Lebanon, CBP denied nine Chinese international students entry at the border.[183] The students, who were returning for their fall semester at Arizona State University (ASU), "were deemed inadmissible to the United States based on information discovered during the CBP inspection."[184] Although the specific reasons for the revocation have not been released, ASU President Michael Crow sent a letter to Secretary of State Mike Pompeo and other government officials expressing concern over the policies that allow warrantless searches of students' electronic devices at the border.[185] While Ajjawi was fortunate to be able to return to the United States in time for the start of classes, the students from China had yet to be granted admission.[186]

The experiences of Ajjawi and the ASU Chinese students, while extreme, are not isolated incidents.[187] Other college administrators have reported recent incidents of border authorities searching incoming student's electronic devices, and

179. *See, e.g.*, *id.* (describing situation with Harvard student adding to anxiety around visa process).

180. *See* Karin Fischer, *Visas Revoked at the Border Put a New Dent in American Higher Ed's Image Abroad*, THE CHRON. OF HIGHER EDUC. (Sept. 4, 2019), https://www.chronicle.com/article/Visas-Revoked-at-the-Border/247074 [https://perma.cc/37YX-9HVV] (detailing cases of Palestinian Harvard student and Chinese ASU students).

181. *See* Svrluga, *supra* note 2 (describing search and reason for entry denial).

182. *See* Dickson, *supra* note 3 (highlighting Ajjawi's statement CBP found no political posts on his social media).

183. *See* Kiara Quaranta, *Nine Returning Chinese ASU Students Denied Entry to the US*, THE STATE PRESS (Sept. 4, 2019, 3:13 AM), https://www.statepress.com/article/2019/09/sppolitics-nine-chinese-students-denied-entry-to-the-us [https://perma.cc/96LG-PC26] (reporting CBP denied entry for nine Chinese students).

184. *Id.*

185. *See id.* (describing concerns ASU president raised).

186. *See* Fischer, supra note 180 (noting Chinese students unable to return to United States).

187. *See id.* (pointing to additional incidents of international students denied at border following electronic search); Wong, *supra* note 18 (acknowledging Ajjawi's situation extreme). While few incoming international students have experienced this type of entry denial, the mere possibility creates concerns and increases anxiety for students and colleges. *See* Wong, *supra* note 18 (noting policy and enforcement changes burdensome to universities).

at least two of those students were denied entry.[188] With so many uncertainties, college leaders worry that the risk of electronic border searches leading to visa revocation could dissuade students from studying in the United States.[189]

III. ANALYSIS

A. Riley *Should Not Be Strictly Applied at the Border*

No court has required a warrant or probable cause for electronic searches at the border, and circuits are split regarding the level of suspicion required for a forensic search of electronic devices at the border.[190] The Supreme Court has not spoken on this issue, but has never required probable cause or a warrant for any type of search at the border, no matter how invasive.[191] The Court's decision in *Riley* did not change the state of affairs at the border.[192] Rather, *Riley* should inform the level of suspicion for electronic searches at the border in order to create a standard that is both appropriate and feasible.[193]

A strict application of *Riley* to border searches would effectively eliminate the border search exception for electronic searches.[194] Instead, *Riley* can serve as a guide for treating electronic data in a manner different from other personal property, but should not be applied strictly in a context that the Court did not consider in its decision.[195] The heightened government interests at the border in

188. *See* Fischer, *supra* note 180 (noting other cases of electronic searches at border). Two students at McNeese State University in Louisiana were recently denied entry based on electronic searches. *See id.* (quoting college administrator's impression of entry denial reasoning "nebulous"). Some colleges asked for anonymity and were unable to share details, making the true extent of the issues unknown. *See id.*

189. *See id.* (detailing concerns of universities). Miriam Feldblum, executive director of the Presidents' Alliance for Higher Education and Immigration, cautioned, "[n]ot knowing what will happen at the border increases fear and anxiety . . . It reinforces doubts and concerns that students may have about studying in the United States." *Id.*

190. *See* Nowell, *supra* note 6, at 96 (noting no warrant requirement for electronic search at border by lower courts); *supra* Section II.D (elucidating circuit split).

191. *See* United States v. Molina-Isidoro, 884 F.3d 287, 292 (5th Cir. 2018) (highlighting absence of post-*Riley* Supreme Court decision requiring warrant for electronic searches at border); DeSimone, *supra* note 25, at 729 (noting highest standard Supreme Court has applied regarding border searches).

192. *See* Nowell, *supra* note 6, at 95-96 (pointing to Court's lack of clarification in border search context). *Riley* did not provide clarification on how the limitations on digital searches should apply in other contexts. *See id.*; Riley v. California, 573 U.S. 373, 401 (2014) (applying holding only in context of search incident to arrest).

193. *See* DeSimone, *supra* note 25, at 729-30 (articulating strict application of warrant requirement for digital data at border impractical); O'Grady, *supra* note 12, at 2280 (arguing *Riley* should "carry weight" in border search context); *see also Riley*, 573 U.S. at 403 (holding warrant required for electronic search incident to arrest); Carroll, *supra* note 50, at 12 (asserting privacy concerns of *Riley* should impact electronic searches at border).

194. *See* Nowell, *supra* note 6, at 101 (cautioning strict application of *Riley* to electronic searches would eliminate exception); *supra* Section II.B.1 (articulating historical justification and purpose of border search exception). Strict application of *Riley* would require a warrant and probable cause for any search of an electronic device, the very requirement the exception eliminates. *Compare Riley*, 573 U.S. at 403 (requiring warrant for digital search), *with supra* Section II.B.1 (discussing rationale behind border search exception).

195. *See Riley*, 573 U.S. at 403 (holding warrant required for electronic search incident to arrest); Carroll, *supra* note 50, at 13 (asserting privacy concerns articulated in *Riley* should affect electronic searches at border).

"protecting this Nation from entrants who may bring anything harmful into this country" make a warrant requirement—for any type of search—impractical and contradictory to the very purpose of the border exception.[196] Additionally, the Court has repeatedly explained that an individual's expectation of privacy is less at the border than in the interior of the country, while the government's interest is "at its zenith at the international border."[197] Changes in technology and what people choose to carry across the border should not diminish the government's heightened interest in protecting its borders.[198]

B. Reasonable Suspicion Should Be Required for Forensic Searches of Electronic Devices at the Border

Although a warrant requirement would not be practical or feasible, forensic searches of electronic devices at the border should require some level of suspicion.[199] Throughout the long history of the Fourth Amendment border exception, the Supreme Court has only determined one type of border interaction that requires reasonable suspicion—detention beyond a routine inspection coupled with an extremely intrusive search of the person.[200] The Court additionally provided examples of two other situations in which a search at the border might not be per se reasonable: destructive searches of property and searches conducted in a "particularly offensive manner."[201] Given this legal backdrop, forensic searches of

196. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 544 (1985) (articulating government's interests at border); DeSimone, *supra* note 25, at 729-30 (explaining impracticability of warrant requirement at border). Requiring a warrant for any search at the border "is more burdensome due to the large volume of items moving across the border with the added difficulty of obtaining a warrant when the subject of the search is mobile." DeSimone, *supra* note 25, at 729. Further, while some states have expedited the process of obtaining warrants through electronic applications, these expedited applications are not available in every state. *See id.* at 730.

197. *See* United States v. Flores-Montano, 541 U.S. 149, 152-53 (2004) (recognizing multiple occasions Court noted government interest greater at border); *Montoya de Hernandez*, 473 U.S. at 539 (noting expectation of privacy less at border); *see also* Carroll v. United States, 267 U.S. 132, 154 (1925) (describing heightened expectation of privacy within nation's borders).

198. *See* United States v. Cotterman, 709 F.3d 952, 987 (9th Cir. 2013) (en banc) (Smith, J., dissenting) (criticizing majority's reliance on changes in technology to alter application of border search exception).

199. *See* Riley v. California, 573 U.S. 373, 393 (2014) (distinguishing digital devices from other personal property); Carroll, *supra* note 50, at 12 (explaining heightened privacy interests does not necessitate warrant requirement); *supra* note 196 and accompanying text (explaining impracticability of warrant requirement at border). *Riley* observed that the "immense storage capacity" of electronic devices distinguishes them from wallets or purses, and border officials should treat them differently. *Riley*, 573 U.S. at 393. Applying this rationale at the border means recognizing the distinguishing features of electronic devices and requiring a slightly higher level of suspicion. *See* Carroll, *supra* note 50, at 12 (describing workable reasonable suspicion standard).

200. *See Montoya de Hernandez*, 473 U.S. at 541-42 (requiring reasonable suspicion for detention of traveler at border beyond routine inspection); *Flores-Montano*, 541 U.S. at 152 (stating "highly intrusive searches of the person" may support further suspicion); *Cotterman*, 709 F.3d at 972, 980 (Smith, J., dissenting) (noting single instance Court required reasonable suspicion for search at border).

201. *See Flores-Montano*, 541 U.S. at 155-56, 154 n.2 (describing two additional circumstances where search possibly deemed unreasonable); *Cotterman*, 709 F.3d at 973 (Smith, J., dissenting) (articulating three situations where search at border possibly not per se reasonable).

electronic devices could be considered "particularly offensive" due to the sensitive nature of the data stored on these devices, therefore requiring reasonable suspicion before such a search.[202]

Requiring reasonable suspicion solely for forensic searches of electronic devices would not undermine the border search exception.[203] The balance between individual privacy rights and government interests would remain "struck much more favorably to the Government."[204] As the *Cotterman* court explained, "[r]easonable suspicion is a modest, workable standard that is already applied in the extended border search . . . and other contexts."[205] When applied to forensic searches, reasonable suspicion "will not impede law enforcement's ability to monitor and secure our borders or to conduct appropriate searches of electronic devices."[206]

Additionally, requiring reasonable suspicion would not create additional national security concerns or administrative burdens.[207] Requiring reasonable suspicion would fall in line with existing CBP policy, which mandates reasonable suspicion for forensic searches of electronic devices, and potentially even reinforce it.[208] CBP officers would retain their authority to conduct manual searches of electronic devices without suspicion, and would only need "a minimal level of objective justification" for a forensic search.[209]

---

202. *See Riley*, 573 U.S. at 392 (cautioning diminished expectation of privacy does not entirely preclude Fourth Amendment protections). *But see Cotterman*, 709 F.3d at 973 (Smith, J., dissenting) (arguing intrusive searches of persons exceptions cannot apply to electronic devices). The Court in *Riley* articulated that "[t]he fact that an [individual] has diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely." *Riley*, 573 U.S. at 392.

203. *See Cotterman*, 709 F.3d at 967 (asserting reasonable suspicion will not undo border search exception or hinder work of border agents); Nowell, *supra* note 6, at 103 (arguing reasonable suspicion should only apply to forensic searches). Manual searches should continue to be allowed without any level of suspicion, but forensic searches should require more. *See Cotterman*, 709 F.3d at 967.

204. United States v. Montoya de Hernandez, 473 U.S. 531, 539-40 (1985) (explaining reasonable suspicion standard still favors government at border).

205. United States v. Cotterman, 709 F.3d 952, 966 (9th Cir. 2013) (en banc) (articulating manageability of reasonable suspicion standard).

206. *Id.* (recognizing no negative impact on ability of law enforcement to secure borders).

207. *See id.* at 966-67 (describing CBP officers' continued ability to protect nation's security). The court in *Cotterman* explained that reasonable suspicion does not create additional burdens, but instead "leave[s] ample room for agents to draw on their expertise and experience to pick up on subtle cues that criminal activity may be afoot," while recognizing Fourth Amendment interests. *Id.* (detailing reasonable suspicion in context of Fourth Amendment).

208. *See* CBP Directive, *supra* note 92, at 5 (requiring reasonable suspicion for forensic search and no suspicion for manual).

209. *See* Illinois v. Wardlow, 528 U.S. 119, 123 (2000) (articulating reasonable suspicion standard); Carroll, *supra* note 50, at 9-10 (arguing no increased burden with reasonable suspicion standard). In his dissent, Judge Smith of the Ninth Circuit expressed concern that mandating a standard of reasonable suspicion "will likely disincentivize agents to conduct [electronic] searches in close cases." *Cotterman*, 709 F.3d at 985 (Smith, J., dissenting). This concern may not be warranted, however, as CBP already mandates this level of suspicion through their internal policies. *See* CBP Directive, *supra* note 92, at 5 (establishing procedures for CBP officers).

As it stands now, CBP officers are unlikely to conduct a lengthy and expensive forensic search without having some level of suspicion of illegal activity.[210] Notwithstanding the circuit split, courts have concluded in many forensic search cases that CBP officers had reasonable suspicion for the electronic searches conducted.[211] There is no evidence that suggests that requiring reasonable suspicion for forensic searches would create a loophole for criminals, or that such a requirement would discourage CBP officers from conducting such searches.[212] If anything, setting a uniform standard would give more authority to the current CBP policy and bolster the decisions made pursuant to it, decreasing litigation.[213]

C. Higher Education Will Suffer if Courts Fail to Establish a Uniform Standard of Suspicion for Forensic Searches

A uniform standard would not only reinforce the current CBP policy, it would also create a level of certainty for international students pursuing an education in the United States.[214] While cases like Ismail Ajjawi's and the ASU students from China are extreme, they had an immediate negative impact on the U.S. higher education system's image overseas.[215] These incidents, where international students are turned away at the border despite holding valid visas, increase "fear and anxiety" and "reinforce[] doubts and concerns that students may have about studying in the United States."[216]

Even prior to these visa denials, colleges and universities reported visa concerns as the top reason for the decline in new international student enrollment.[217] Similarly, schools that have not yet seen a decline in new international student enrollment have reported that they have had to increase their efforts to recruit international students.[218] With the rise of electronic searches at the border, more

---

210. *See Cotterman*, 709 F.3d at 967 n.14 (noting limited resources make suspicionless forensic search unlikely); O'Grady, *supra* note 12, at 2283 (noting rarity of forensic searches). *See generally* DHS ASSESSMENT, *supra* note 103, at 6 (describing policy requiring level of suspicion for forensic searches).

211. *See* United States v. Touset, 890 F.3d 1227, 1237 (11th Cir. 2018) (holding agents had reasonable suspicion); United States v. Kolsuz, 890 F.3d 133, 147-48 (4th Cir. 2018) (concluding CBP officers did not conduct search absent suspicion); United States v. Cotterman, 709 F.3d 952, 969-70 (9th Cir. 2013) (en banc) (noting CBP officers had reasonable suspicion to conduct search).

212. *See Cotterman*, 709 F.3d at 966 (stating reasonable suspicion does not impede law enforcement's ability to protect border); Carroll, *supra* note 50, at 11 (noting no evidence of negative impact).

213. *See* CBP Directive, *supra* note 92, at 5 (requiring reasonable suspicion prior to forensic examination); Carroll, *supra* note 50, at 11 (predicting fewer lawsuits and "better-informed" agents).

214. *See* Fischer, *supra* note 180 (discussing uncertainty caused by visa revocation following electronic searches at border); *supra* Section II.B.3.b (elucidating current CBP policy).

215. *See* Fischer, *supra* note 180 (reporting immediate impact on higher education's reputation in United States); Wong, *supra* note 18 (noting situations like Harvard and ASU students extreme).

216. Fischer, *supra* note 180 (stressing impact on international students and educators). These types of situations have also caused anxiety in educators, administrators, and presidents at colleges and universities. *See id.*; Wong, *supra* note 18 (discussing concerns university presidents and administrators reported).

217. *See* Wong, *supra* note 18 (citing results of 2017-2018 survey).

218. *See id.* (noting some colleges not yet seeing declines). The President of Franklin and Marshall College reported that visa issues, combined with political tensions, have required the school to "take extraordinary

international students will be subject to such searches when entering the country for school.[219] The detrimental effects of increased searches may not be immediate but will likely lead to a decline in international student enrollment, resulting in decreased diversity at U.S. colleges and universities and a lasting economic impact on higher education in the United States.[220]

While the United States has traditionally been the top destination for international students, competition from other countries has increased.[221] The United States' competitive edge for international students may decline where other countries present fewer hurdles and less uncertainty for students obtaining visas and in gaining entry into those countries.[222] Losing its status as a primary destination for international students could result in dire consequences for higher education and the United States economy.[223] Creating a greater degree of certainty for international students by requiring reasonable suspicion for forensic searches would improve the image of the United States as a destination for higher education and halt the decline in enrollment.[224]

IV. CONCLUSION

The border search exception to the Fourth Amendment is vital to maintaining the security of the United States, but that does not mean it should remain unchanged. The Supreme Court can recognize the history and function of the border search exception while still accounting for new privacy concerns brought on by the ever-increasing use of electronic devices. In *Riley*, the Supreme Court acknowledged the heightened privacy concerns regarding cell phone searches and limited the search incident to arrest exception by requiring a warrant for searches of electronic devices. While a warrant requirement at the border would be impractical, *Riley* should inform the Supreme Court on how to determine the level of suspicion necessary to conduct a forensic search of an electronic device at the border.

---

measures . . . so international students know [they're welcome here]." *Id.* Other colleges have created programs in which current students reach out to incoming international students to reassure them about coming to the United States to study. *See id.*

219. *See supra* Section II.B.3 (discussing rise in electronic searches at border).

220. *See* Fischer, *supra* note 180 (elucidating immediate impact on higher education); *see also supra* Section II.E.1 (discussing international students' significant positive impact on U.S. economy and higher education).

221. *See* SANGER & BAER, *supra* note 176, at 6 (noting global competition one cause of decline). Global competition is among the top two reasons cited for the decline in new international student enrollment in the United States, with many colleges and universities noting Canada's increased recruitment of international students. *See id.*

222. *See generally supra* Section II.E (discussing various impacts on numbers of international students in United States).

223. *See supra* Section II.E.1 (discussing international students' financial contribution to U.S. economy and higher education).

224. *See* Fischer, *supra* note 180 (discussing need for improved perception of studying in United States); Wong, *supra* note 18 (giving overview of issues colleges and universities face).

The Supreme Court's silence has resulted in the current circuit split and the potential that individuals entering the United States will be subjected to suspicionless searches of their phones and computers. The lack of a set standard and government accountability has also impacted international students attempting to enter the United States, resulting in reputational and financial consequences for U.S. higher education. International students already face numerous uncertainties when going through the visa process, and incidents like those faced by the Harvard and ASU students only increase international students' anxiety about studying in the United States.

The Supreme Court should establish a uniform standard of reasonable suspicion for forensic searches of electronic devices at the border. Requiring reasonable suspicion would not hinder the important task of securing the borders and would not undermine the border search exception; rather, it would ensure the accountability of government action. Such a standard would also create a level of certainty for international students planning to study in the United States, which is necessary to protect the reputation, diversity, and financial interests of institutes of higher education in the United States.

Ashley Veronica Hart