Privacy at the Border: Applying the Border Search Exception to Digital Searches at the United States Border

Laura Nowell *

TABLE OF CONTENTS

* J.D., May 2019, The George Washington University Law School; B.A., History and Political Science, May 2015, Presbyterian College. Senior Notes Editor, *Federal Communications Law Journal*, 2018 – 19. Thank you to the staff of the Federal Communications Law Journal (the "FCLJ") and to Sherwin Siy, FCLJ Journal Adjunct for their contributions and assistance with publication.

I. INTRODUCTION

In 2016 alone, eighty million people traveled outbound across the United States[1] and seventy-five million people traveled inbound through the United States.[2] As millions of people cross the United States border each year and the relevance of electronic devices for continuous everyday use increases, digital searches at the border become increasingly common. According to United States Customs and Border Protection ("CBP"), CBP Agents searched electronic devices belonging to 14,993 individuals entering or exiting through the United States border out of 189.6 million individuals traveling through the United States in 2017.[3] With the significant increase in the number of digital searches at the border, the need to determine the standard of suspicion required for conducting digital searches by Border Patrol and Transportation Security Administration officers at the border has also exponentially increased. With cases like *Alasaad v. Duke* in the District of Massachusetts being brought at the district court level against the Department of Homeland Security with the claim of Fourth Amendment violations for the search and seizure of electronic devices at the border without probable cause or a warrant, the discussion at hand in this Note remains at the forefront of current constitutional issues not yet decided by the Supreme Court.[4]

This Note addresses whether the border search exception to the Fourth Amendment should apply to both physical and digital searches at the border. First, Part II will provide a brief general background on the Fourth Amendment's balance between government protection and individual privacy rights and will discuss several exceptions to the Fourth Amendment. Part III will then discuss the standard for a digital search set by the Supreme Court in *Riley v. California* and will analyze why the Court set a different standard for digital searches than for searches of physical evidence in searches incident to lawful arrest.[5] Part IV will analyze why *Riley* is not applicable to border searches. Part V will discuss why the border search exception should be applied to both physical and digital searches at the United States border and proposes that the Supreme Court should adopt the Ninth and Fourth Circuit standard, which holds that an examination of the difference between forensic and manual digital searches at the border should be utilized as the factor to determine whether a digital search constitutes an especially intrusive search.

---

1. *U.S. Resident Travel to International Destinations Increased Eight Percent in 2016*, INT'L TRADE ADMIN. (Dec. 4, 2017), https://travel.trade.gov/outreachpages/download_data_table/2016_Outbound_Analysis.pdf. [https://perma.cc/7NNL-JEHR].

2. *2016 Monthly Tourism Statistics*, NTTO, https://travel.trade.gov/view/m-2016-I-001/table1.asp.

[https://perma.cc/5SKV-MXAW] (last visited Oct. 26, 2018).

3. *CBP Releases Statistics on Electronic Device Statistics*, UNITED STATES CUSTOMS AND BORDER PROTECTION (Apr. 11, 2017), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0 [https://perma.cc/N2KU-FJ3G] [hereinafter *CBP Releases Statistics on Electronic Device Statistics*].

4. *See* Amended Complaint at 1-2, Alasaad v. Duke, No. 1:17-cv-11730-DJC (D. Mass. Sept. 13, 2017), https://www.aclu.org/legal-document/alasaad-v-duke-complaint [https://perma.cc/NXX9-YDHE].

5. *See* Riley v. California, 134 S. Ct. 2473, 2493 (2014).

Part VI will conclude that by examining manual versus forensic digital searches, the Court will maintain the balance, which the Court first established in *Montoya de Hernandez*, between the government interest to provide national security, control of the borders, and the individual privacy interest.[6]

II. BACKGROUND

The Fourth Amendment provides the fundamental right to security and privacy from intrusion by the government by protecting an individual's security in their person and their belongings through prohibiting unreasonable searches and seizures.[7] Two separate clauses comprise the Fourth Amendment: the reasonableness clause and the warrant clause.[8] While the reasonableness clause requires that a search and seizure be reasonable, the warrant clause requires probable cause in order for a warrant to be granted.[9] The warrant must meet the particularity requirement by being supported with a particularized description of "the place to be searched" and the "people or things to be seized."[10]

Although a warrant is required to search a person or their property, the Supreme Court has upheld several exceptions that allow for a warrantless search and seizure under the Fourth Amendment.[11] The Court has established exceptions to the Fourth Amendment right because the Court has consistently held that the interest of the government must be balanced with the protection of an individual's privacy.[12] The Supreme Court established the Fourth Amendment balancing test known as the special needs doctrine in *Terry v. Ohio* and held that "a search is Constitutional where the government's interest in preventing crime outweighs the individual's interest in privacy."[13] The special needs doctrine is an exception to the Fourth Amendment, where the Court gives the government interest a "boost" in overcoming the interest of individual privacy rights in the balancing test.[14] In 2009, the Supreme Court continued to emphasize the importance of balancing these two interests by holding in *United States v. Villamonte-Marquez* that the search must be

6. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985).

7. U.S. CONST. amend. IV.

8. *See* William Clark, *Protecting the Privacies of Digital Life: Riley v. California, the Fourth Amendment's Particularity Requirement, and Search Protocols for Cell Phone Search Warrants*, 56 B.C. L. REV. 1981, 1986 (2015) (citations omitted).

9. *See id.* (citations omitted).

10. *See id.* (internal quotation marks omitted).

11. *See* Parker Jenkins, *OMG Not Something to LOL About: The Unintended Results of Disallowing Warrantless Searches of Cell Phones Incident to a Lawful Arrest*, 31 BYU J. PUB. L. 437, 441 (2017); *see also* Almeida-Sanchez v. United States, 413 U.S. 266, 274 (1973); Katz v. United States, 389 U.S. 347, 357 (1967).

12. *See* Alison M. Lucier, *You Can Judge a Container by Its Cover: The Single-purpose Exception and the Fourth Amendment*, 76 U. CHI. L. REV. 1809, 1809 (2009); *see also Almeida-Sanchez*, 413 U.S. at 274.

13. *See* Ari B. Fontecchio, *Suspicionless Laptop Searches Under the Border Search Doctrine: The Fourth Amendment Exception that Swallows Your Laptop*, 31 CARDOZO L. REV. 231, 233 (2009); Terry v. Ohio, 392 U.S. 1, 1 (1968).

14. *See* Fontecchio, *supra* note 14, at 233.

judged by "balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests."[15]

A. The Single Purpose Container Exception

The single purpose container exception, which allows a warrantless search of an item because the container's use is clear prior to search, is a key exception to the warrant requirement that falls within the larger category of the plain view exception.[16] Under the plain view exception, if the contents of the container are in plain view and known prior to search, there is a lowered expectation of privacy.[17] The warrantless search of the container is permissible if the container is so "distinctive that its contents are a foregone conclusion," and the contents are therefore considered to be in plain view.[18] A circuit split exists regarding how the determination of the single purpose container should be made.[19] While the Ninth and Tenth Circuits have consistently held that an objective viewpoint should be applied, the Fourth and Seventh Circuits have held that a subjective viewpoint should be applied.[20]

The Ninth and Tenth Circuits hold that the "objective viewpoint of a reasonable person" should be utilized to determine if the item subject to search constitutes a single purpose container.[21] In *United States v. Miller*, the Ninth Circuit held that neither the circumstances of the discovery of the evidence nor the expertise of the officer who discovered the evidence should be utilized to determine if the item constitutes a single purpose container.[22] In *Miller*, the Ninth Circuit held that the DEA agents, who conducted a warrantless search of a bag that was not transparent and lacked a distinctive shape and odor, conducted a search in violation of the defendant's Fourth Amendment right because the container was not so "distinctive that its contents" of a controlled substance were not a "foregone conclusion."[23] The Tenth Circuit, in *United States v. Bonitz*, declined to expand the single-purpose container exception to include "qualities independent of the container surrounding the search," because the court feared that extending the exception to these circumstances "would permit officers to conduct a 'warrantless search of any container found in the vicinity of a suspicious item.'"[24] However, the Fourth Circuit held that the officer's subjective viewpoint should be utilized, and the officer should account for the container's surrounding circumstances.[25] The Fourth Circuit in *United States v. Williams*

15. *See* United States v. Miller, 769 F.2d 554, 560 (9th Cir. 1985); United States v. Donnes, 947 F.2d 1430, 1438 (10th Cir. 1991).
16. *See* Lucier, *supra* note 13, at 1809.
17. See *id.*
18. *See id.* at 1817-18 (citation omitted).
19. *Id.* at 1809.
20. *See id.*
21. *See* United States v. Miller, 769 F.2d 554, 560 (9th Cir. 1985); United States v. Donnes, 947 F.2d 1430, 1438 (10th Cir. 1991); Lucier, *supra* note 13, at 1820-21.
22. *See Miller*, 769 F.2d at 560; *see also* Lucier, supra note 13, at 1820-21.
23. *See* Lucier, *supra* note 13, at 1809; *see also Miller*, 769 F.2d at 560.
24. *See* Lucier, *supra* note 13, at 1822 (citing Bonnitz v. United States, 826 F.2d 954, 956 (10th Cir. 1987)).
25. *See* Lucier, *supra* note 13, at 1826.

held that the subjective viewpoint should be applied because "the circumstances under which an officer finds the container may add to the apparent nature of its contents."[26]

B. The Exigent Circumstances Exception

In addition, there is an exigent circumstance exception to the Fourth Amendment, which allows a warrantless search and seizure to be conducted when both a time pressure exists and the evidence is at risk of being lost or destroyed.[27] In *Riley v. California*, the Supreme Court held that "police cannot search information on an arrestee's cell phone without a warrant, unless exigent circumstances exist at the time of the arrest" and that the "exigency must 'make the needs of law enforcement so compelling that the warrantless search is objectively reasonable under the Fourth Amendment.'"[28] According to the Court, "exigency is both situational and environmentally influenced" based on "reasonableness, present needs, and existing facts."[29] The Supreme Court defined the standard required for exigent circumstances in *Brigham City v. Stuart* as requiring the officer to possess an objectively reasonable basis to believe that "someone was seriously injured or imminently threatened with such injury."[30]

C. The Search Incident to Lawful Arrest Exception

The search incident to lawful arrest creates a balancing test between the "reasonableness of a warrantless search, with the basic rule that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.'"[31] The Supreme Court established the search incident to lawful arrest exception to the Fourth Amendment in the holding for *Mapp v. Ohio*.[32] The Court held later in *United States v. Robinson* that the primary purpose of the search incident to lawful arrest exception was to protect the government interest of providing for both the safety of officers and providing for the

---

26. *See id.* at 1823.

27. *See* Di Jia et al., *An Analysis and Categorization of U.S. Supreme Court Cases Under the Exigent Circumstances Exception to the Warrant Requirement*, 27 GEO. MASON U. CIV. RTS. L.J. 37, 40-41 (2016) (citation omitted).

28. *Id.* at 41-42, (citing Mincey v. Arizona, 437 U.S. 385, 394 (1978)).

29. *See* Di Jia et al*., supra* note 28, at 42 (internal citations omitted) (internal quotation marks omitted); *see also* Graham v. Connor, 490 U.S. 128, 138 (1990) (finding that "[d]etermining whether the force used to effect a particular seizure is "reasonable" under the Fourth Amendment requires a careful balancing of 'the nature and quality of the individual's Fourth Amendment interests' against the countervailing governmental interests at stake."); Kentucky v. King, 563 U.S. 452, 452 (2011) (holding that the need to prevent destruction of evidence invoked the exigent circumstances doctrine and justified the warrantless entry).

30. *See* Di Jia et al., *supra* note 28, at 42 (citing Brigham City v. Stuart, 547 U.S. 398, 400 (2006)).

31. Arizona v. Gant, 556 U.S. 332, 338 (2009) (quoting Katz v. United States, 389 U.S. 347, 357 (1967)).

32. *See Gant*, 556 U.S. at 393; *see also* Mapp v. Ohio, 367 U.S. 643, 644 (1961); United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985).

preservation of evidence.[33] The Court later limited the search incident to arrest exception to only include "the arrestee's person and the area 'within his immediate control'—construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence."[34] The purpose for this restriction by the Court was to ensure that the government's interest to protect officers and to protect evidence susceptible to being destroyed following arrest would be maintained while also limiting the infringement that the exception causes on the Fourth Amendment rights of the individual.[35]

The Supreme Court also placed further restrictions on the search incident to lawful arrest exception by finding in *Preston v. United States* that "if there is no possibility that an arrestee could reach into the area that law enforcement officers seek to search, both justifications for the search-incident-to-arrest exception are absent and the rule does not apply."[36] In *Riley v. California*, the Supreme Court further restricted the search incident to lawful arrest exception by holding that the exception did not apply to searches of electronic devices, specifically referring to cell phone data, and only applied to physical searches. [37] The Supreme Court made a crucial distinction between digital and physical searches when the Court held in *Riley* that a warrant is required for digital searches incident to lawful arrest unless an emergency exists, and that the search incident to lawful arrest exception does not apply to forensic or manual digital searches of cell phone data, although the purposes of protecting the officer and the evidence still apply in digital searches.[38]

D. The Border Search Exception

The Supreme Court has also consistently held that the Fourth Amendment's "balance of reasonableness is qualitatively different at the international border than in the interior."[39] The Court held in *Montoya de Hernandez* that "since the founding of our Republic, Congress has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country."[40] In *United States v. Ramsey*, the Court held that the lower expectation of privacy at the borders exists because the state has a compelling interest to control "who and what may enter the country." [41] The Court also held in *Ramsey* that "a 'reasonable cause to suspect' a customs law violation . . . is 'a practical

33. United States v. Robinson, 414 U.S. 218, 230 (1973).
34. *Gant*, 556 U.S. at 335 (internal quotations omitted).
35. *See id.* at 335.
36. *See* Preston v. United States, 376 U.S. 364, 368; *see also Gant*, 556 U.S. at 335.
37. *See* Riley v. California, 134 S. Ct. 2473, 2493 (2014).
38. *See id.* at 2494.
39. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 535 (1985).
40. *See id.* at 537 (citations omitted).
41. *See* United States v. Ramsey, 431 U.S. 606, 606 (1977); Victoria Wilson, *Laptops and the Border Search Exception to the Fourth Amendment: Protecting the United States Borders from Bombs, Drugs, and the Pictures from Your Vacation*, 65 U. MIAMI L. REV. 999, 1003 (2011).

test,' less stringent than the probable cause standard for the issuance of warrants imposed by the Fourth Amendment." [42]

The motivation for the state's interest in lowering the expectation of privacy at the United States borders has transformed over time from a purely financial interest to an interest in providing for the national security and to preventing the trafficking of illegal contraband across the border.[43] In 1985, the Supreme Court held in *United States v. Montoya de Hernandez* that "concern for the protection of the border is heightened by veritable national crisis in law enforcement caused by smuggling of illicit narcotics."[44] Additionally, the Court established the parameters of the border exception in *Montoya de Hernandez* by holding that a search at the border requires neither a warrant, probable cause, nor reasonable suspicion so that the search may uncover evidence or contraband.[45] If the search constitutes an especially intrusive search, the Court held that probable cause would be required.[46] For the purposes of the border search exception, the border is defined as an "international boundary," and the Court held in *Almeida-Sanchez v. United States* that "agents are acting within the Constitution when they stop and search automobiles without a warrant, without probable cause . . . to believe the cars have made a border crossing" when the individuals are within a reasonable distance from the border.[47]

Since *Ramsey*, the Court has significantly expanded the border exception from requiring the "reasonable cause to suspect" to a lower standard of permitting searches at the border based on suspicion at any level.[48] In 2004, a few years after the September 11th attacks, the Supreme Court continued to expand the border search exception by finding in *United States v. Flores Montano* that "the Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border."[49] The Supreme Court bolstered the importance of the weight of the government interest in searches at the border by holding that "searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border."[50]

---

42. *See* Gretchen C. F. Shappert, *The Border Search Doctrine: Warrantless Searches of Electronic Devices after Riley v. California*, 62 U.S. ATT'YS BULL. 1, 2 (2014), https://www.justice.gov/sites/default/files/usao/legacy/2014/11/14/usab6206.pdf [https://perma.cc/C5CA-U8FN]; *see Ramsey*, 431 U.S. at 606.

43. Wilson, *supra* note 42, at 1004-05.

44. *See id.*

45. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 535 (1985).

46. *See id.*

47. *See* Almeida-Sanchez v. United States, 413 U.S. 266, 274 (1973) (holding that officers could search travelers in a car twenty miles from the border without violating their Fourth Amendment rights because "travelers may be stopped in crossing an international boundary because of national self-protection").

48. *See* Wilson, *supra* note 42, at 1004.

49. *See* United States v. Flores Montano, 541 U.S. 149, 152 (2004); *see also* Fontecchio, *supra* note 14, at 233.

50. *See Flores Montano*, 541 U.S. at 152; *see also* Wilson, *supra* note 42, at 233.

Within the border search exception, the Court has generally distinguished between routine and non-routine searches.[51] While a routine search constitutes a less intrusive search through methods such as pat downs, surveillance through metal detectors, and requiring the emptying of individuals' pockets, searches characterized in the category of routine require no level of suspicion of criminal activity.[52] If reasonable suspicion of an illegal activity such as smuggling contraband exists, a non-routine search may be conducted.[53] The courts have characterized searches including destruction of objects, use of prolonged detention, strip searches, body cavity searches, and x-ray searches as non-routine searches.[54]

E. Differences Between Forensic and Manual Digital Searches

When officers conduct searches of electronic data, there are five levels of digital evidence extraction techniques.[55] Manual extraction represents the most basic level of the techniques used to gain evidence from an electronic device and allows access only to information available by "point-and-click" operations.[56] This most basic level of extraction does not require any use of special tools and only allows the searcher to access information on the "standard interface" with no access to deleted items or clusters of deleted items available through this process.[57] The "point-and-click" method of searching is comparable to "sitting at a computer looking for a particular file by exploring file folders with a mouse and keyboard."[58] Beyond the basic manual search, the National Criminal Justice Reference Services established four levels of forensic search, all of which require specialized tools and knowledge to conduct.[59] These four levels of invasive data extraction include in order of increasing complexity: logical extraction, physical extraction, chip-off extraction, and micro read extraction.[60] The logical extraction process "incorporates external computer equipment to provide commands through code to the targeted device" and accesses information and data that would not be accessible through "simply point and click" methods.[61] The physical extraction process provides access to the flash memory, where a device stores the history of actions on the device, and provides access to deleted information that is not available through "point and click" or through logical extraction.[62] Both the chip-off extraction process and

51. *See* Stephen R. Vina et al., *Protecting our Perimeter: "Border Searches" Under the Fourth Amendment*, CRS (Aug. 15, 2006), http://trac.syr.edu/immigration/library/P1075.pdf [https://perma.cc/3BPW-9H3T].
52. *See id.*
53. *See id.*
54. *See id.* (citations omitted).
55. *See* Sean E. Goodison et al., *Digital Evidence and the U.S. Criminal Justice System*, NAT'L INST. OF JUSTICE (2014), https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf [https://perma.cc/TGC4-Y77U].
56. *See id.*
57. *See id.*
58. *See id.*
59. *See id.*
60. *See id.*
61. *See id.*
62. *See id.*

the micro read process require highly technical knowledge and equipment to extract data directly from the memory chip and not through the device, so the search is similar to a microscopic search of the information.[63] Each level of digital extraction provides access to increasing amounts of evidence not accessible in a basic manual search including deleted file clusters.[64] Throughout each of the four levels of forensic extraction, the information from the device available significantly increases in quantity and increases in difficulty for the suspect to alter.[65] The chip-off and micro read extraction techniques constitute a "microscopic examination" of the contents of the digital device and is therefore by far the most invasive form of extraction.[66]

III. THE SUPREME COURT STANDARD SET IN RILEY V. CALIFORNIA: DIGITAL SEARCHES IN INCIDENT TO LAWFUL ARREST

In *Riley v. California*, the Supreme Court established that the standard for a digital search incident to arrest is categorically different than the standard for a physical search incident to arrest.[67] The Court rejected the government's argument that an electronic device containing digital information is analogous to a physical container that is subject to search in the same situation.[68] The Supreme Court held that the "search incident to arrest exception to the warrant requirement does not apply to cell phones" and that a constitutional search may occur without a warrant following an arrest under certain exceptions: to preserve evidence, to pursue a fleeing suspect, and to help those injured or in imminent danger.[69] The Court held that the search of the defendant's phone violated his Fourth Amendment right to be free from an unreasonable search because cell phones are distinguishable from other physical items that are subject to search on a person due to the quantity and quality of the information stored on the electronic device itself and the information that can be accessed on the phone but is stored on remote servers.[70] Due to the significant amount of private information stored on the phone and due to the information stored on remote servers through the "cloud" not being considered legally on the phone, the Court held that the phone therefore could not be subject to a warrantless search.[71] According to the Court, the warrantless searches of cell phones could be conducted in the instance of an emergency, if the search could be deemed reasonable based on the government's interest.[72] The Court explained a balancing test in *Riley* that

63. *See id.*
64. *See id.*
65. *See id.*
66. *See id.*
67. *See* Riley v. California, 134 S. Ct. 2473, 2493 (2014).
68. *See id.* at 2478.
69. *Id.* at 2494.
70. *See id.* at 2490-91.
71. *See id.*
72. *See id.* at 2494; *see also* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 663-65 (1995) (holding that a reasonable government interest to provide for the safety of minors who participate in high school athletics through random drug testing existed and outweighed the intrusion of the student athletes' Fourth Amendment rights); Shappert, *supra* note 43.

weighed the government's interest against the level of intrusion to the individual's privacy to determine what circumstances require deviation from the warrant requirement.[73] However, the Court left the appropriate level of suspicion required unclear and instead, chose to "expressly reserve the question."[74] The Court also held in *Riley* that digital searches constitute a non-routine search but did not address whether the traditional border search exception excludes digital searches at the border from this rule.[75]

The Supreme Court originally distinguished between routine and non-routine searches in *United States v. Montoya de Hernandez*.[76] In *Montoya de Hernandez*, the Court explained that under *Ramsey*, that "routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant."[77] The Court limited routine searches in *Montoya de Hernandez* to apply to border searches, which are "'reasonably related in scope to the circumstances which justified it initially.'"[78] Also, the Court in *Riley* did not address the level of suspicion for non-routine border searches, which the Court defined in *Montoya de Hernandez* as overly intrusive searches such as strip searches, body cavity searches, or involuntary x-ray searches.[79]

Although the Supreme Court held in *Riley* that digital searches are distinct from physical searches during searches incident to lawful arrest, the Court did not address whether the standard set in *Riley* applies to and places limitations on the border search exception for digital searches at the border.[80] The Court in *Riley* did not comment on whether digital and physical searches require different standards when applying the border exception.[81] In addition, although *Riley* provides a balancing test, the Court left the answers to several key questions unclear.[82] First, the Supreme Court has not discussed whether a heightened expectation of privacy exists for encrypted digital information or password protected information.[83] Second, the Court did not address whether manual searches and forensic searches, which provide access to significantly different qualities and quantities of evidence, should require a different level of suspicion by border patrol agents. or whether a heightened expectation of privacy therefore exists.[84] Because *Riley* addresses neither the border exception nor the substantial differences in quality and quantity of information accessible between manual and forensic digital searches, the Department of Homeland Security has not applied *Riley* to border search directives.[85] DHS does not instruct border patrol agents to treat electronic

73. *See* Riley v. California, 134 S. Ct. 2473, 2493 (2014).
74. Thomas M. Miller, *Digital Border Searches after Riley v. California*, 90 WASH. L. REV. 1943, 1995 (2015).
75. *See id.*
76. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985).
77. *See* Miller, *supra* note 75, at 1957 (citing United States v. Ramsey, 431 U.S. 606 (1977) (internal quotation)).
78. *See* Miller, *supra* note 75, at 1957.
79. *See id.* at 1958.
80. *See* Riley v. California, 134 S. Ct. 2473, 2493 (2014).
81. *See* Miller, *supra* note 75, at 1945.
82. *See generally Riley*, 134 S. Ct. at 2493; *see also* Miller, *supra* note 75, at 1945.
83. *See generally Riley*, 134 S. Ct. at 2493; *see also* Miller, *supra* note 75, at 1945.
84. *See generally Riley*, 134 S. Ct. at 2493; *see also* Miller, *supra* note 75, at 1945.
85. *See Riley*, 134 S. Ct. at 2493; *also see* Miller, *supra* note 75, at 1945.

devices as distinct from physical containers and therefore does not consider the standard required for suspicion to be any higher for a digital search than for a physical search at the border.[86]

IV. WHY *RILEY V. CALIFORNIA* SHOULD NOT BE APPLIED TO DIGITAL BORDER SEARCHES BROADLY

Although *Riley* provides no clarification on whether the same limitations placed on domestic digital searches subject to lawful arrest apply also to digital searches at the United States border, the Supreme Court has provided some clarification through consistently distinct holdings for searches incident to arrest and border exception searches. The Supreme Court has consistently held that searches incident to arrest are limited with respect to closed containers but also has consistently held that searches lacking any suspicion are permitted under the border search exception.[87] Lower courts seeking to answer the standard of suspicion necessary for digital searches at the border have varied in their approaches, which has led to a circuit split.[88] Although the majority of lower courts have required reasonable suspicion for a non-routine search, these courts have typically defined a non-routine search based on the level of intrusiveness of the search.[89] No lower courts have held that a digital border search that falls within the border search exception requires a warrant, and the United States Customs and Border Protection's authority to conduct such warrantless searches has been consistently upheld.[90]

A. The Ninth and Fourth Circuit Test for Digital Searches at the Border: Manual v. Forensic Digital Searches

Lower courts have divided in a split, with the Ninth Circuit and Fourth Circuits holding that the courts should apply the border exception to digital searches at the border by utilizing the balancing test between the government's interest and the of level intrusiveness based upon whether Border Patrol officers conducted a forensic or a manual digital search.[91] However, the United States District Court for the District of Columbia held that the court should instead treat all digital and physical searches at the border as inherently different and therefore not allow digital border searches without some heightened level of suspicion present under the border exception.[92] According to the Ninth and Fourth Circuits, border agents may conduct manual digital searches without a warrant, probable cause, or reasonable

86. *See* Miller, *supra* note 75, at 1950 (internal citations omitted).
87. *See id.* at 1945.
88. *Id.*
89. *See* United States v. Cotterman, 709 F.3d 952, 960 (9th Cir. 2013); *see also* United States v. Ickes, 393 F.3d 501, 505 (4th Cir. 2005); *see also* United States v. Arnold, 533 F.3d 1003, 1009 (9th Cir. 2008).
90. *See Cotterman*, 709 F.3d at 960; *Ickes*, 393 F.3d at 505; *Arnold*, 533 F.3d at 1009; *see also CBP Releases Statistics on Electronic Device Statistics*, *supra* note 4.
91. *See Cotterman*, 709 F.3d at 960; *see also Ickes*, 393 F.3d at 505; *see also Arnold*, 533 F.3d at 1009; *see also* United States v. Kim, No. 13-cr-00100-ABJ, 2015 BL 134375 (D.D.C. May 8, 2015).
92. *See also Kim*, No. 13-cr-00100-ABJ, 2015 BL 134375.

suspicion under the border exception, but agents are prohibited from conducting forensic searches, which always constitute an overly intrusive search, without reasonable suspicion of uncovering evidence or contraband.[93] The Ninth Circuit held in the *United States v. Cotterman* that Border Patrol Agents must possess "reasonable suspicion of criminal activity" to justify a forensic digital search of a laptop at the border but not for a manual search.[94]

CBP also directs officers that they may search, read, retain, copy, and share private data from a laptop searched under the border exception at the United States border.[95] These actions may be taken by border patrol on computer hard drives and external data storage units, and officers may retain the data for an "indeterminate amount of time."[96] CBP states that it adjusts its search procedures and directives to align with the current "threat information" while following constitutional and statutory authority.[97]

The Ninth and Fourth Circuits have not held that all digital searches at the border are non-routine nor constitute an overly intrusive search under the border search exception to the Fourth Amendment.[98] Instead, both circuits have applied the border exception established in *Montoya de Hernandez* to both physical and digital searches at the border and have analyzed the level of intrusiveness of the digital searches by distinguishing between manual and forensic digital searches.[99]

In *United States v. Cotternman*, the Ninth Circuit recognized the significant increase in quantity of information and deleted information that can be attained from remote servers during a forensic search, which cannot also be attained in a manual search.[100] The quantity and quality of the information attainable only through a forensic search constitutes an overly intrusive border search according to the Ninth Circuit.[101] In *United States v. Arnold***,** the Ninth Circuit held that a digital search of a laptop at the border does not require reasonable suspicion, and the court rejected the argument that the search of a laptop is analogous to the search of a home despite providing access to large quantities of evidence.[102] The court held that no distinction

93. *See Cotterman*, 709 F.3d at 956-957; *see also Ickes*, 393 F.3d at 504-05; *see also* Miller, *supra* note 75, at 1972-75.

94. *See* Miller, *supra* note 75, at 1946; *see also Ninth Circuit Holds Forensic Search of Laptop Seized at Border Requires Showing of Reasonable Suspicion*, 127 HARV. L. REV. 1041, 1041 (2014) (citing) (internal quotation marks omitted).

95. *See* Fontecchio, *supra* note 14, at 232 (citation omitted).

96. *See id.* (citation omitted).

97. *See CBP Releases Statistics on Electronic Device Searches, supra* note 4.

98. *See* United States v. Cotterman, 709 F.3d 952, 961 (9th Cir. 2013); *see also* United States v. Ickes, 393 F.3d 501, 505 (4th Cir. 2005); *see also* United States v. Arnold, 533 F.3d 1003, 1009 (9th Cir. 2008); *see also* United States v. Kim, No. 13-cr-00100-ABJ, 2015 BL 134375 (D.D.C. May 8, 2015).

99. *See Cotterman*, 709 F.3d at 956-957; *see also Ickes*, 393 F.3d at 504-05.

100. *See Cotterman*, 709 F.3d at 956-957.

101. *See id* at 982.

102. *See Arnold*, 533 F.3d at 1008-09.

exists between a warrantless and suspicion-less border search of luggage from a similar search of a laptop.[103]

The Fourth Circuit in *United States v. Ickes* also rejected limitations of electronic border searches and rejected the argument that searches of computers at the border should be limited based on the quality of information stored.[104] In *Ickes*, the court held that the presence of speech which might implicate First Amendment concerns does not implicate limitations on a border search.[105] The court in the Southern District of Maryland also distinguished between forensic and manual searches in *United States v. Saboonchi*, where the court held that reasonable suspicion was required for a forensic search when Border Patrol agents seized hard drives at the border to be subject to a forensic search at a later time.[106] The court held that such a forensic search would expose "intimate details" of the defendant's private affairs through the forensic extraction of some browsing histories and deleted files that would not be available through a manual digital search.[107] The Fourth Circuit then decided in 2018 in *United States v. Kolsuz* that border patrol agents must acquire a probable cause warrant before conducting a forensic digital search at the border.[108] The court stipulated that the holding did not apply to manual digital searches and found that "the distinction between manual and forensic searches is a perfectly manageable one."[109]

B. The District Court for the District of Columbia's Application of Riley v. California to Border Search Cases

The United States District Court for the District of Columbia, in *United States v. Kim*, applied *Riley* to the digital border search broadly and found that *Riley* applies to the search of electronic devices in all circumstances including both manual and forensic searches.[110] In *Kim*, TSA agents searched and seized the defendant's laptop and DHS subsequently searched the laptop's hard drive and extracted thousands of documents using specialized software but obtained a warrant for the extracted data only after the fact.[111] The District Court for the District of Columbia found in *Kim* that the *Riley* Court "made it clear that the breadth and volume of data stored on computers and other smart devices make today's technology different."[112] As a result, the burden is increasingly higher for the government to establish a compelling

---

103. *See id.* at 1008-09 (holding that customs officers were permitted to search the contents of a passenger's laptop with no reasonable suspicion of the passenger being involved in a customs violation or criminal activity); *see also* Cooper Offenbecher, *Border Searches of Laptop Computers after United States v. Arnold: Implications for Traveling Professionals*, 5 SHIDLER J. L. COM. & TECH. 9 (2008).

104. *See Ickes*, 393 F.3d at 504-05 (holding that no level of suspicion was required to search a computer at the border in a manual digital search).

105. *See id.* at 506-507.

106. *See* United States v. Saboonchi, 990 F.Supp.2d 536, 548 (D. Md. 2014).

107. *See id* at 553.

108. United States v. Kolsuz, 890 F.3d 133, 146 (4th Cir. 2018).

109. *See id.*

110. *See* United States v. Kim, No. 13-cr-00100-ABJ, 2015 BL 134375, at *36-37 (D.D.C. May 8, 2015).

111. *Id.* at 1.

112. *Id.* at 34.

interest that outweighs the "degree to which the search intrudes upon an individual's privacy."[113]In *Kim*, the court chose not to address whether the Court's limitation in *Riley* on a digital search incident to lawful arrest should be distinguished from a limitation on a border search of an electronic device.[114] By not acknowledging this difference, the District Court for the District of Columbia failed to recognize the distinct purposes and parameters set for the border search exception in *Montoya de Hernandez* and the search incident to lawful arrest exception under *Arizona v. Gant*, where the Supreme Court held that "the exception derives from interests in officer safety and evidence preservation that are typically implicated in arrest situations."[115] The two exceptions are inherently different, and the search subject to lawful arrest exception has been limited by the Court significantly more than the border search exception.[116] While the border search exception was created for significantly different and broad purposes by the Court to support the government's interest in protecting the borders and providing for the national security, the search subject to lawful arrest exception was created for the purpose of protecting the officer involved in the arrest and search and to protect the evidence that is tied to the arrest at hand from being destroyed.[117]

Therefore, the two exceptions should be treated differently by the Court in regard to searches of electronic devices just as the Supreme Court has treated the two exceptions differently in physical searches.[118] As a result, *Riley* should not be applied by the Court to digital searches at the border because in *Riley*, the Court intended to restrict the search incident to lawful arrest but did not address the border search exception.[119] Furthermore, the differentiation of digital and physical searches for searches subject to lawful arrest that *Riley* established does not necessarily apply to digital searches at the border.

V. THE BORDER SEARCH EXCEPTION SHOULD BE APPLIED TO BOTH PHYSICAL AND DIGITAL SEARCHES AT THE UNITED STATES BORDER

The Supreme Court established the border search exception to provide the government with an advantage because the government's interest in regulating what enters and exits the country outweighs the individual interest of privacy in a majority of instances.[120] The increasing presence of persons carrying digital devices that store electronic information across borders does not create a shift in the balance of the government's interest

113. *Id.* at 36; *see also* Miller, *supra* note 75, at 1975 (internal quotation marks omitted).

114. *See Kim*, No. 13-cr-00100-ABJ, 2015 BL 134375, at *29.

115. *See* Arizona v. Gant, 556 U.S. 332, 338 (2009); United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985).

116. *See* Mapp v. Ohio, 367 U.S. 643, 644 (1961); *see also Montoya de Hernandez*, 473 U.S. at 541.

117. *See Mapp*, 367 U.S. at 644; *see also Montoya de Hernandez*, 473 U.S. at 541; *see also* Miller, *supra* note 75, at 1946; *see also* Riley v. California, 134 S. Ct. 2473, 2493 (2014).

118. *See* Miller, *supra* note 75, at 1946; *see also Riley*, 134 S. Ct. at 2488-89, 2493.

119. *See Riley*, 134 S. Ct. at 2485.

120. *See* Almeida-Sanchez v. United States, 413 U.S. 266, 274 (1973).

versus individual privacy interests. On the contrary, this increase in portable technology provides the opportunity to more efficiently, quickly, and more frequently commit crimes across the border, such as the trafficking of drugs, humans, and other illegal contraband.[121] The Supreme Court first established the border search exception in the interest of controlling trade and subsequently, in the interest of preventing the rapidly increasing flow of drugs into the United States.[122] Since the September 11th terrorist attacks, the government's interest in monitoring the border has increasingly stemmed from the need to provide for national security and to thwart growing threats of terrorism.[123]

A. Applying the Original Intent of the Border Search Exception v. the Original Intent of the Search Incident to Lawful Arrest

By recognizing the important difference between a forensic search of an electronic device and a manual search, the Court will not deviate from the border exception's original intent and standard set by the Supreme Court in *Montoya de Hernandez*.[124] The government interest will receive heightened protection while individuals' privacy interests will continue to receive the same level of protection guaranteed by the Court in *Montoya de Hernandez* because the Court will continue to require reasonable suspicion for overly intrusive searches.[125] The forensic digital search can reach significantly more information located on remote servers and in flash memory, which is not accessible through "point and click" methods.[126] Therefore, the amount of information available through forensic methods is more analogous to an overly intrusive search as defined by *Montoya de Hernandez* and less analogous to a routine physical search.[127] Searching an electronic device for large quantities of evidence in the flash memory, in deleted storage, and on remote servers is more analogous to the search of a home because the evidence constitutes a large quantity of potentially more sensitive information, and therefore a heightened expectation of privacy should be associated with both the search of a home and a forensic electronic search.[128] In *Montoya de Hernandez*, the Supreme Court held that the rectal search of an individual suspected of trafficking drugs into the United States by smuggling the contraband by hiding it in her alimentary canal did not constitute an overly intrusive search.[129] The Court found in *Montoya de Hernandez* that "the fact that protection of the public might, in the abstract, have been accomplished by 'less intrusive' means does not, in itself, render the search unreasonable."[130] Under *Montoya de Hernandez*, the Court set a

121. *See* Richard Davis & Ken Pease, *Crime, Technology, and the Future*, 13 SECURITY J. 59, 61 (2009).
122. *See* Wilson, *supra* note 42, at 1003-04.
123. *See id.*
124. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985).
125. *See id.*
126. *See* Goodison, *supra* note 56.
127. *See Montoya de Hernandez*, 473 U.S. at 541.
128. *See* Miller, *supra* note 75, at 1946.
129. *See Montoya de Hernandez*, 473 U.S. at 541.
130. *See id.* (citations omitted).

high bar for proving that a search constitutes an overly intrusive search,[131] and under this standard, a forensic search is more analogous to this definition of an overly intrusive search than a manual "point and click" search.[132]

B. The Exigent Circumstances Exception as an Alternative Justification for Warrantless Digital Searches at the Border

In opposition to applying the border search exception to all searches at the border in the same manner, the dissent in *Montoya de Hernandez* argues for requiring reasonable suspicion for a search that "involves such severe intrusions on the values the Fourth Amendment protects that more stringent safeguards are required" because some "border detentions may involve the use of such highly intrusive investigative techniques as body-cavity searches, x-ray machines, and stomach-pumping."[133] The dissent here argues that there are many instances in which the border exceptions do not provide a heightened government interest for national security at the border that outweighs the Fourth Amendment rights of individuals.[134] As an alternative to the border protection exception, the exigent circumstances exception provides the justification for the warrantless search of electronic devices at the border.

Proponents within this school of thought who advocate for requiring a warrant for all electronic searches at the border and for extending *Riley*'s holding to border searches have filed suit in the United States District Court for the District of Massachusetts in *Alasaad v. Duke* on behalf of eleven plaintiffs who underwent searches of their laptops and cell phones by CBP officers and Immigration and Customs Enforcement Officers when crossing the United States border.[135]

The proponents who advocate for effectively eliminating the border search exception for all digital searches and who are in favor of requiring probable cause or a warrant to conduct all digital searches at the border fail to recognize that the exigent circumstances exception also applies at the border in many instances.[136] The exigent circumstances exception provides the justification for manual digital searches at the border without probable cause or a warrant because the government's interest to control the borders to provide for national security creates the necessary situational circumstances for the exigency exception to apply.[137] The exigent circumstances exception is applied based on "situational and environmentally influenced" circumstances based on "reasonableness, present needs, and existing facts."[138] The Supreme Court held in *Brigham City, Utah v. Stuart* that the exigent circumstances exception provides the justification for warrantless searches

131. *See id.*
132. *See* Goodison, *supra* note 56.
133. *See Montoya de Hernandez*, 473 U.S. at 551-52 (Brennan, J. dissenting).
134. *See id.*
135. *See* Amended Complaint, Alasaad v. Duke, No. 1:17-cv-11730-DJC at 1 (D. Mass. Sept. 13, 2017).
136. *See* Jia, *supra* note 28, at 38.
137. *See id.* at 41-42.
138. *Id.* at 42 (internal citations omitted) (internal quotation marks omitted).

when an objectively reasonable basis for the search exists to prevent someone from being seriously injured.[139]

When heightened levels of threats to national security persist at the border, CBP officers and TSA officers must adjust search procedures based on the current "threat information."[140] The knowledge of an imminent threat to public safety creates the circumstances necessary to invoke the exigent circumstances and justifies a search without a warrant, probable cause, or reasonable suspicion.[141] If the officer bases the search upon reasonableness and the present need for heightened security to provide for the safety of persons imminently in danger according to the existing facts, then manual digital searches are subject to the exigent circumstances exception to the Fourth Amendment.[142] In such circumstances, the interest of the national government outweighs the individual privacy interest.[143] Similarly, the Court held in *Riley*, when referring to a domestic digital search not at the border, that exigent circumstances must be "so compelling that [a] warrantless search is objectively reasonable," but when officers possess knowledge of heightened national security threats, the warrantless manual digital search is objectively reasonable.[144] However, the forensic search that requires an extensive period of time, expertise, and equipment to conduct as well as the ability to retain significantly more information[145] would likely not be held by the Court as being justified by the exigent circumstances exception.

C. Case Study: Alasaad v. Duke

In the pending district court case, *Alasaad v. Duke*, the plaintiffs echo the D.C. District Court's holding in *Kim*, in construing *Riley* to stand for the proposition that digital and physical searches are categorically different, and therefore, the exceptions to the Fourth Amendment should not be applied equally for each but rather should be extended and applied to the border exception as well.[146] The plaintiffs in *Alasaad* argue that the border search exception established in *Montoya de Hernandez* should be applied to only physical searches at the border and exclude digital border searches.[147] The plaintiffs do not distinguish between manual and forensic searches in their argument and do not claim that the officers conducted forensic searches on the electronic devices in question but only mention that many forensic searches are conducted by border patrol agents.[148] The plaintiffs in *Alasaad* claim that if the District Court for the District of Massachusetts applied *Riley*, all of the digital searches at the border in question would be violations of the

139. *See* Brigham City v. Stuart, 126 S. Ct. 1943, 1946 (2006); Jia, *supra* note 28, at 40.
140. *See CBP Releases Statistics on Electronic Device Statistics, supra* note 4.
141. *See id.*
142. *See Stuart*, 547 U.S. at 402-03; Jia, *supra* note 28, at 40.
143. *See Stuart*, 547 U.S. at 402-03; Jia, *supra* note 28, at 40.
144. *See* Riley v. California, 134 S. Ct. 2473, 2493 (2014) (internal citations omitted) (internal quotation marks omitted).
145. *See* Goodison, *supra* note 56.
146. *See* Amended Complaint at 38, Alasaad v. Duke, No. 1:17-cv-11730-DJC (D. Mass. Sept. 13, 2017); Goodison, *supra* note 56.
147*See* Amended Complaint at 38, Alasaad v. Duke, No. 1:17-cv-11730-DJC (D. Mass. Sept. 13, 2017).
148. *See id.*

Fourth Amendment because the officers conducting the searches lacked probable cause or a warrant.[149] However, if the district court applies *Riley* to *Alasaad*, the court would extend *Alasaad* beyond the scope of search incident to arrest and would fail to acknowledge the differences in the purposes of the search incident to arrest exception and the border search exception.

Instead of applying *Riley* and effectively eliminating the border search exception, which no Circuit Court has yet done, the United States District Court for the District of Massachusetts should apply the Ninth and Fourth Circuit standard to *Alasaad v. Duke*.[150] By applying the Ninth Circuit holding from *United States v. Cotterman* to *Alasaad*, the district court would recognize the significant increase in quantity of information and quality of information in a forensic search, which creates a heightened expectation of privacy that is not present in the evidence available in a "point and click" manual search.[151] Due to the heightened expectation of privacy from access to deleted information and information on remote servers through a forensic search, the District Court in *Alasaad* should hold that forensic searches and manual searches cannot be considered equally when examining whether the government overly intruded an individual's privacy rights.[152] The district court should hold as the Court did in *United States v. Arnold* that forensic searches require reasonable suspicion while manual digital searches at the border do not, which would balance the government's interest in providing for the national security with the personal privacy interest of the individuals traveling across the United States border.[153]

The plaintiffs in *Alasaad* argue that they possess a heightened expectation of privacy because some of their electronic devices, which were searched at the border without a warrant under the justification of the border exception to the Fourth Amendment, contained sensitive work-related material. [154] However, the Fourth Circuit held in *United States v. Ickes* that searches of computers at the border should not be limited based on the quality of information stored.[155] The District Court in *Alasaad* should apply the Fourth Circuit's holding in *Ickes* because Ickes' concern that the information stored on his electronic device that was searched by border patrol agents at the border implicated First Amendment concerns is analogous to the claims of the plaintiffs in *Alassad* that their digital information should be protected with a heightened expectation of privacy.[156] The district court in *Alassad* should, as the Fourth Circuit did in Ickes, "refuse to undermine" the "well-settled law by restrictively reading the statutory language in 19 U.S.C. §

149. *See id.* at 56.

150. *See* United States v. Cotterman, 709 F.3d 952, 955 (9th Cir. 2013); *see also* United States v. Arnold, 533 F.3d 1003, 1009 (9th Cir. 2008); *see also* United States v. Ickes, 393 F.3d 501, 505 (4th Cir. 2005).

151. *See Cotterman*, 709 F.3d at 955.

152. *See id.* at 967.

153. *See Arnold*, 533 F.3d at 1008.

154. *See* Amended Complaint at 38, Alasaad v. Duke, No. 1:17-cv-11730-DJC (D. Mass. Sept. 13, 2017).

155. *See Ickes*, 393 F.3d at 505-06.

156. *See id.*

1581(a) or by carving out a First Amendment exception to the border search doctrine."[157]

VI. CONCLUSION

As electronic devices continuously grow in their capacities to contain significant amounts of personal information and as travel across the United States border also continues to exponentially grow each year, the significance and relevance of the border search exception's application to digital searches remains at the forefront of Fourth Amendment issues. *Riley* should not be applied broadly to all digital searches because each search exception to the Fourth Amendment originated with a distinct intent, and extending *Riley* beyond its application to the search incident to lawful arrest exception sets the precedent of treating all exceptions to the Fourth Amendment exactly alike. Instead, the Supreme Court should instead adopt the holding of the Ninth and Fourth Circuits to provide for the most equal balance between the government's interest to control the borders and individuals' Fourth Amendment rights by broadly applying the border exception to manual searches but requiring a heightened level of suspicion for forensic digital searches at the border.

157. *See id.* at 502.