ALL WATCHED OVER BY MACHINES OF LOVING GRACE: BORDER SEARCHES OF ELECTRONIC DEVICES IN THE DIGITAL AGE

*Sean O'Grady**

The border search exception to the Fourth Amendment has historically given the U.S. government the right to conduct suspicionless searches of the belongings of any individual crossing the border. The federal government relies on the border search exception to search and detain travelers' electronic devices at the border without a warrant or individualized suspicion.

The government's justification for suspicionless searches of electronic devices under the traditional border search exception for travelers' property has recently been called into question in a series of federal court decisions. In March 2013, the Ninth Circuit in United States v. Cotterman *became the first federal circuit court to rule that a border search of an electronic device may require reasonable suspicion that its owner committed a crime due to the privacy impact of such a search. The following year, in* Riley v. California *(a nonborder search case), the U.S. Supreme Court explicitly endorsed the view that searches of cell phones implicate privacy concerns far beyond those implicated by searches of other physical items. Most recently, two divergent circuit court decisions,* United States v. Kolsuz *and* United States v. Touset*, lay bare the conflict in the federal circuit courts between a view that border searches of electronic devices are no different than those of other personal property and an emerging sense that digital border searches merit additional scrutiny due to their increased likelihood to harm travelers' Fourth Amendment privacy interests.*

This Note proposes that courts should extend the logic of Riley *to the border by treating searches of travelers' electronic devices as distinctly more harmful to Fourth Amendment interests than searches of other types of property. This Note argues that border searches of electronic devices should be justified by a standard of at least reasonable suspicion in order to balance the necessity of border searches with the adverse impact on Fourth*

* J.D. Candidate, 2020, Fordham University School of Law; B.A., 2012, Reed College. Thank you to Professor Ian Weinstein and the editors and staff of the *Fordham Law Review* for their tireless assistance and sage advice. I would also like to thank my family, friends, and Thea for their encouragement and support.

Amendment privacy concerns caused by extensive searches of travelers' digital devices.

INTRODUCTION

In July 2017, two U.S. citizens traveling from Canada to Vermont were detained by U.S. Customs and Border Protection (CBP) officers while crossing the border.[1] Customs officers gave no reason for the search: a CBP supervisor told the travelers that they were being detained and that their smartphones were being searched because he "simply felt like ordering a secondary inspection."[2] One of the travelers, who wears a headscarf in accordance with her religious beliefs, refused to give a male CBP officer permission to search her phone because it contained photographs of her

1. Alasaad v. Nielsen, No. 17-cv-11730-DJC, 2018 WL 2170323, at *5 (D. Mass. May 9, 2018).
2. *Id.*

without her headscarf.[3] After approximately six hours of detention, the travelers departed without their phones, which were returned damaged fifteen days later.[4]

A 2009 CBP policy in force at the time of these border searches permitted "confiscation of electronic devices for on- or off-site search without any level of suspicion."[5] Recognizing this, law enforcement officials have ordered border searches of travelers' devices to gather evidence of crimes unrelated to the import or export of contraband.[6] This policy has forced certain travelers—including lawyers who need to protect attorney-client privilege, business people with proprietary information, researchers who promise their subjects anonymity, and photojournalists who may pledge to blur a face to conceal an identity—to take precautions to minimize data on electronic devices they take across the U.S. border.[7]

The border search doctrine, which dates back to this country's founding era, exempts government searches of travelers' belongings from the traditional Fourth Amendment protections against warrantless searches and seizures.[8] The U.S. Supreme Court has repeatedly justified this exemption by reasoning that "the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity."[9] The long-standing border search doctrine permits extensive, intrusive, suspicionless searches of property at the border—but places limits on invasive searches of a traveler's body.[10]

The government routinely conducts suspicionless searches of travelers' electronic devices at the border in accordance with the traditional border search doctrine.[11] Federal courts initially rejected Fourth Amendment

---

3. *See id.*

4. The traveler contended that CBP's search and seizure of one phone "damaged its functionality." *See id.*

5. *See id.* (noting that "the 2009 CBP Policy did not distinguish between a basic and advanced search and no level of suspicion was required for either").

6. *See, e.g.*, United States v. Jae Shik Kim, 103 F. Supp. 3d 32, 46 (D.D.C. 2015) (describing a law enforcement officer's border search of a traveler's laptop as "nothing more than a fishing expedition to discover what [the traveler] might have been up to").

7. *See* David K. Shipler, *Can You Frisk a Hard Drive?*, N.Y. TIMES (Feb. 19, 2011), https://www.nytimes.com/2011/02/20/weekinreview/20laptop.html [https://perma.cc/3X45-U3NE].

8. United States v. Ramsey, 431 U.S. 606, 617–18 (1977).

9. United States v. Flores-Montano, 541 U.S. 149, 153 (2004); *see also* United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985); *Ramsey*, 431 U.S. at 616–17.

10. *Compare Flores-Montano*, 541 U.S. at 154–56 (upholding the suspicionless disassembly of a car's fuel tank), *with Montoya de Hernandez*, 473 U.S. at 541 (holding that the extended, nonroutine detention of a traveler at the border was justified by customs officers' reasonable suspicion that the traveler was smuggling drugs in a body cavity).

11. *See, e.g.*, Mana Azarmi & Greg Nojeim, *Border Searches of Electronic Devices: Oh, the Places Your Data Will Go*, CTR. FOR DEMOCRACY & TECH. (Sept. 17, 2018), https://cdt.org/blog/border-searches-of-electronic-devices-oh-the-places-your-data-will-go/ [https://perma.cc/XW6E-CWBZ]; Sophia Cope & Aaron Mackey, *New CBP Border Device Search Policy Still Permits Unconstitutional Searches*, ELECTRONIC FRONTIER FOUND. (Jan. 8, 2018), https://www.eff.org/deeplinks/2018/01/new-cbp-border-device-search-policy-still-permits-unconstitutional-searches [https://perma.cc/6WL4-UZFU].

challenges to border searches of electronic devices on the grounds that cell phones and computers are no different than other forms of property.[12] More recent cases suggest the emergence of a view that searches of electronic devices implicate Fourth Amendment privacy interests more than searches of other types of personal property.[13] In 2013, the Ninth Circuit held in *United States v. Cotterman*[14] that the Fourth Amendment requires border agents to show reasonable suspicion of criminal activity before undertaking a "forensic" search of a computer.[15] In *Riley v. California*,[16] a nonborder decision issued the following year, the Supreme Court explicitly rejected the view that searches of cell phones should be treated the same as searches of other types of property. In *Riley*, a unanimous Court declared that searches of "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[17] Following *Cotterman* and *Riley*, a split emerged in the circuit courts over whether to extend *Riley*'s privacy-focused treatment of electronic devices to the border.[18]

Millions of people cross the United States border carrying cell phones and electronic devices every day.[19] On a typical day in the 2017 fiscal year, American border officials processed 1,088,300 incoming passengers and pedestrians, including 283,664 private vehicles.[20] The vast majority of Americans—95 percent—own a cell phone, with 77 percent of Americans now owning a smartphone.[21] Nearly all of those travelers carried a

12. *See, e.g.*, United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008) (holding that the Fourth Amendment does not protect electronic devices—including computers and cell phones—from warrantless and suspicionless searches in the border context); United States v. Ickes, 393 F.3d 501, 504–05 (4th Cir. 2005) (same); *see also* United States v. Linarez-Delgado, 259 F. App'x 506, 508 (3d Cir. 2007) (stating that there is no reasonable suspicion required for a routine border search of "[d]ata storage media and electronic equipment, such as films, computer devices, and videotapes").

13. *See* Thomas Mann Miller, Comment, *Digital Border Searches After* Riley v. California, 90 WASH. L. REV. 1943, 1979–82 (2015).

14. 709 F.3d 952 (9th Cir. 2013) (en banc).

15. *Id.* at 956–57.

16. 134 S. Ct. 2473 (2014).

17. *Id.* at 2488–89.

18. *See infra* Part II.

19. *See* Patrick G. Lee, *Can Customs and Border Officials Search Your Phone? These Are Your Rights*, PROPUBLICA (Mar. 13, 2017, 12:55 PM), https://www.propublica.org/article/can-customs-border-protection-search-phone-legal-rights [https://perma.cc/85LK-2GLN].

20. *On a Typical Day in Fiscal Year 2017, CBP . . .*, U.S. CUSTOMS & BORDER PROTECTION (Feb. 13, 2018), https://www.cbp.gov/newsroom/stats/typical-day-fy2017 [https://perma.cc/82X8-RHGT]. In all, approximately 226.9 million air passengers traveled between the United States and the rest of the world in 2017. *See* U.S. DEP'T OF TRANSP., U.S. INTERNATIONAL AIR PASSENGER AND FREIGHT STATISTICS 3 (2017), https://www.transportation.gov/sites/dot.gov/files/docs/mission/office-policy/aviation-policy/311371/us-international-air-passenger-and-freight-statistics-december-2017_0.pdf [https://perma.cc/SLS9-L3BA] (noting a 5 percent increase in passengers from the previous year).

21. *Mobile Fact Sheet*, PEW RES. CTR. (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/mobile/ [https://perma.cc/7J7M-N4P3] (noting that the smartphone figure is up from just 35 percent since 2011). In fact, approximately 90 percent of U.S. households contain at least one internet-connected electronic device (smartphone, desktop or laptop computer, tablet, or

smartphone or laptop,[22] which means that nearly all of those devices were subject to warrantless, suspicionless searches by U.S. border officials.[23]

Customs officers stationed at the U.S. border and at airports searched an estimated 30,200 cell phones, computers, and other electronic devices of people entering and leaving the United States in 2017—an almost 60 percent increase from 2016.[24] In fact, U.S. border officials searched more phones in a single month of 2017 than in all of 2015.[25] CBP officials claim that border searches of electronic devices "are critical to the detection of evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography."[26] Privacy activists and those who have been detained at the border say the examination of phones, computers, and hard drives is invasive and violates Fourth Amendment protections against unreasonable searches.[27]

This Note addresses the application of the border search exception to electronic devices.[28] The Supreme Court has not yet decided how Fourth Amendment protections apply to this situation.[29] Based on the traditional border search exception to Fourth Amendment protection, border officials may conduct "routine" searches of persons and personal property without suspicion of criminal activity or a warrant.[30] The Court has indicated that some "nonroutine" searches—including those destructive to personal

---

streaming media device), with the median American household containing five of them. *See A Third of Americans Live in a Household with Three or More Smartphones*, PEW RES. CTR. (May 25, 2017), http://www.pewresearch.org/fact-tank/2017/05/25/a-third-of-americans-live-in-a-household-with-three-or-more-smartphones/ [https://perma.cc/7NR6-CJZV].

22. PORTABLE ELEC. DEVICES AVIATION RULEMAKING COMM., RECOMMENDATIONS ON EXPANDING THE USE OF PORTABLE ELECTRONIC DEVICES DURING FLIGHT H-8 (2013), https://www.faa.gov/about/initiatives/ped/media/PED_ARC_FINAL_REPORT.pdf [https://perma.cc/Q2E4-4A7B] (noting that "[n]early all (94%) U.S. adult airline passengers have brought at least one [portable electronic device] with them onto an aircraft while traveling in the past 12 months").

23. *See generally, e.g.*, *Border Security: America's Front Line* (Force Four Entertainment 2018) (depicting numerous warrantless border searches of cell phones by U.S. customs officers over the course of a twenty-eight-episode reality television series).

24. Ron Nixon, *Cellphone and Computer Searches at U.S. Border Rise Under Trump*, N.Y. TIMES (Jan. 5, 2018), https://www.nytimes.com/2018/01/05/us/politics/trump-border-search-cellphone-computer.html [https://perma.cc/JGH8-NP5Q].

25. *See* 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 [http://perma.cc/3ysc-wcav].

26. Olivia Solon, *US Border Agents Are Doing 'Digital Strip Searches'. Here's How to Protect Yourself*, GUARDIAN (Mar. 31, 2017), https://www.theguardian.com/us-news/2017/mar/31/us-border-phone-computer-searches-how-to-protect [https://perma.cc/Z69N-KVCZ]. Electronic devices "can also reveal information about financial and commercial crimes, such as those relating to copyright, trademark and export control violations." *Id.*

27. *See, e.g.*, Azarmi & Nojeim, *supra* note 11; Nixon, *supra* note 24.

28. This Note will not distinguish between the Fourth Amendment rights or privacy expectations of U.S. citizens and noncitizens at the border.

29. *See infra* Part I.B.; *see also* Miller, *supra* note 13, at 1944–45.

30. *See* Miller, *supra* note 13, at 1944–45.

property or highly intrusive to personal dignity—may require some level of suspicion.[31]

This Note analyzes the two alternative approaches taken by federal circuit courts to the border search exception as it applies to electronic devices.[32] The traditional approach treats border searches of cell phones or other electronic devices as analytically equivalent to searches of physical items that require no individualized suspicion to search.[33] Other courts emphasize the special privacy concerns presented by suspicionless searches of electronic devices and call for a narrower application of the border search exception to digital devices.[34] The circuit split has adverse consequences for customs officials working at airports and border crossings across the United States: whether a border guard needs reasonable suspicion to search your electronic devices depends on where you enter the country.[35]

Part I of this Note provides background information on the nature of the Fourth Amendment's traditional warrant requirement and its border search exception. This breakdown considers recent Supreme Court rulings regarding Fourth Amendment rights at the border.

Part II analyzes the current conflict among the U.S. courts of appeals in how the border search exception should be applied to travelers' now-ubiquitous electronic devices. The Note divides the courts into two groups: (1) those holding that the heightened privacy implications of a nonroutine border search of a traveler's electronic device call for some form of individualized suspicion, and (2) those advocating the traditional position that searches of property at the border may be conducted without any individualized suspicion.

Part III argues that *Riley* endorses a burgeoning understanding of electronic devices as a special category of property subject to heightened privacy concerns. This Note argues that all border searches of electronic devices are therefore nonroutine and require some form of individualized suspicion. This Note concludes by offering several legal and public policy justifications for extending *Riley*'s logic to the border and (partially) endorses the Fourth and Ninth Circuits' understanding of the border search doctrine as it applies to electronic devices.

I. THE FOURTH AMENDMENT AND PRIVACY AT THE BORDER

Though many issues involved in searches of electronic devices are new, the border search exception itself dates back to the country's founding era. This Part reviews the case law underpinning the traditional border search

31. *See infra* Part I.B.1.

32. *See infra* Part II.

33. *See infra* Part II.B; *see also infra* Part I.B.

34. *See* United States v. Kolsuz, 890 F.3d 133, 137 (4th Cir. 2018); United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013) (en banc); *infra* Part II.A.

35. *See* Ayako Hobbs, Tara Swaminatha & Thomas Zeno, *Circuits Split About Border Search of Electronic Devices*, ANTICORRUPTION BLOG (June 19, 2018), https://www.anticorruptionblog.com/data-protection-privacy/circuits-split-about-border-search-of-electronic-devices/ [https://perma.cc/ZQT9-DHTQ].

doctrine and the application of border search principles to electronic devices. It also details recent developments in electronic privacy jurisprudence that may impact the search of digital devices at the border.

A. The Fourth Amendment

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[36] The Fourth Amendment applies when an individual demonstrates a subjective expectation of privacy and society recognizes that expectation as reasonable.[37]

In order for a search or seizure to satisfy the Fourth Amendment, it must be "reasonable."[38] "A search or seizure is ordinarily unreasonable" in the absence of "individualized suspicion of wrongdoing"; the police cannot simply search an individual's house or car at random.[39] A reasonable search "generally requires the obtaining of a judicial warrant" supported by probable cause.[40] According to ordinary Fourth Amendment jurisprudence, a search or seizure accomplished without a judicial warrant issued upon a showing of probable cause is per se unreasonable.[41]

In the absence of a warrant, a search or seizure is reasonable only if it falls within a specific exception to the warrant requirement.[42] The Supreme Court imposes a presumptive warrant requirement for searches and seizures[43] and generally requires probable cause for a warrantless search or seizure to be "reasonable."[44] There are a number of important exceptions to this general warrant requirement, and in practice many searches are conducted without a warrant or probable cause.[45]

Courts have interpreted the Fourth Amendment to permit certain types of searches and seizures as exceptions to the warrant requirement.[46] Advances

---

36. U.S. CONST. amend. IV.

37. *See* Bond v. United States, 529 U.S. 334, 338 (2000) ("Our Fourth Amendment analysis embraces two questions. First, we ask whether the individual, by his conduct, has exhibited an actual expectation of privacy . . . . Second, we inquire whether the individual's expectation of privacy is 'one that society is prepared to recognize as reasonable.'" (quoting Smith v. Maryland, 442 U.S. 735, 740 (1979))).

38. *See* Riley v. California, 134 S. Ct. 2473, 2482 (2014) ("[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness.'" (quoting Brigham City v. Stuart, 547 U.S. 398, 403 (2006))).

39. City of Indianapolis v. Edmond, 531 U.S. 32, 37 (2000).

40. *Riley*, 134 S. Ct. at 2482 (quoting Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995)).

41. *See* United States v. Place, 462 U.S. 696, 701 (1983).

42. *See Riley*, 134 S. Ct. at 2482; Kentucky v. King, 563 U.S. 452, 460 (2011).

43. *See* Katz v. United States, 389 U.S. 347, 357 (1967); *see also* Johnson v. United States, 333 U.S. 10, 14–15 (1948) (noting that the Fourth Amendment requires a warrant for searches and seizures unless a preexisting exception applies).

44. *See, e.g.*, Missouri v. McNeely, 569 U.S. 141, 143 (2013); *Katz*, 389 U.S. at 357; *Johnson*, 333 U.S. at 14–15.

45. *See, e.g.*, City of Los Angeles v. Patel, 135 S. Ct. 2443, 2451–52 (2015); Arizona v. Gant, 556 U.S. 332, 338 (2009); Thompson v. Louisiana, 469 U.S. 17, 19–20 (1984).

46. *See, e.g. Riley*, 134 S. Ct. at 2494; *Katz*, 389 U.S. at 357 & n.19.

in technology brought challenges to the warrant requirement to the Supreme Court.[47] Even in these exceptional cases, the Supreme Court generally requires the government to demonstrate probable cause[48] or a lower standard called "reasonable suspicion"[49] in order for the search to be considered reasonable.[50] Warrantless searches are typically justified when the process of obtaining a judicial warrant would be impracticable or counterproductive to the government's interests.[51]

B. The Border Search Exception

Border searches have historically been viewed as one exception to the individualized-suspicion requirement.[52] Routine border searches are permitted absent any individualized suspicion because "the Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border."[53] However, more intrusive, nonroutine searches may require a showing of a lower level of individualized suspicion: reasonable suspicion.[54]

1. History of the Border Search Exception

Border searches are among the earliest recognized exceptions to the Fourth Amendment requirements of a warrant and probable cause.[55] The same Congress that passed the Fourth Amendment passed the Act of July 31, 1789, which allowed border officials to conduct warrantless searches of vessels entering the United States.[56]

---

47. *See generally Katz*, 389 U.S. 347 (analyzing the Fourth Amendment implications of electronic eavesdropping); Carroll v. United States, 267 U.S. 132 (1925) (discussing the Fourth Amendment implications of an automobile search).

48. *See* Ker v. California, 374 U.S. 23, 34–35 (1963) (stating that a warrantless seizure must be supported by probable cause to believe that the person has committed the violation in question).

49. *See* United States v. Arvizu, 534 U.S. 266, 273 (2002); Illinois v. Wardlow, 528 U.S. 119, 123 (2000); Terry v. Ohio, 392 U.S. 1, 37 (1968).

50. *See Carroll*, 267 U.S. at 155–56 (noting that probable cause is a "reasonableness" standard for warrantless searches and seizures); *see also* Florida v. Royer, 460 U.S. 491, 498 (1983) ("[C]ertain seizures are justifiable under the Fourth Amendment if there is articulable suspicion that a person has committed or is about to commit a crime."); Hill v. California, 401 U.S. 797, 804 (1971) ("[S]ufficient probability, not certainty, is the touchstone of reasonableness under the Fourth Amendment.").

51. *See, e.g.*, Arizona v. Gant, 556 U.S. 332, 338 (2009); Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 618–20 (1989); *Terry*, 392 U.S. at 20.

52. United States v. Ramsey, 431 U.S. 606, 616–18 (1977).

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

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

55. The power of customs officials to conduct searches at the border has an "impressive historical pedigree." United States v. Villamonte-Marquez, 462 U.S. 579, 585 (1983); *see also Ramsey*, 431 U.S. at 616–18; Carroll v. United States, 267 U.S. 132, 150 (1925); Boyd v. United States, 116 U.S. 616, 623–24 (1886).

56. *See Carroll*, 267 U.S. at 150 ("As [the Act of July 31, 1789] was passed by the same Congress which proposed for adoption the original amendments to the Constitution, 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.").

This Act established a series of customs offices and gave 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" and to secure any such items that were found.[57] The Act specifically differentiated between searches conducted on ships at ports of entry—where "full power and authority" were directly granted without need for judicial oversight—and those of "any particular dwelling-house, store, building, or other place" for which the agents needed to obtain a warrant.[58] Therefore, searches at the border could be conducted at the discretion of the customs agents, whereas searches by customs agents for smuggled goods at nonborder locations were subject to an external warrant requirement. This waiver of the warrant requirement at the border is the core of the border search exception, and it has been in place since 1789.[59] The Supreme Court has repeatedly pointed to the long history of the border search exception as support for its constitutionality.[60]

Traditionally, searches conducted at the border or its "functional equivalent"[61] do not require any suspicion on the theory that the government has a strong sovereign interest in regulating what enters and exits the country.[62] The Supreme Court has repeatedly described the federal government's right and obligation to protect the nation's borders in absolutist terms.[63] The Fourth Amendment does not require warrants for routine stops and searches at borders because the sovereign state and its public officials[64]

57. Act of July 31, 1789, § 24, 1 Stat. 29, 43, *repealed by* Act of Aug. 4, 1790, § 74, 1 Stat. 145, 178.

58. *Id.*

59. *See Montoya de Hernandez*, 473 U.S. at 537–38.

60. *See, e.g.*, *Ramsey*, 431 U.S. at 616–17 (noting that the First Congress also proposed the Bill of Rights, and that the First Congress therefore can be presumed not to have thought the Act inconsistent with the Fourth Amendment); *Boyd*, 116 U.S. at 623 (observing that "the seizure of goods forfeited for a breach of the revenue laws . . . has been authorized by English statutes for at least two centuries past").

61. International airports are included as "functional equivalents" of the border. *See, e.g.*, United States v. Irving, 452 F.3d 110, 123 (2d Cir. 2006) (holding that the border search exception applies at international airports because it is the "functional equivalent of a border"); United States v. Yang, 286 F.3d 940, 944 (7th Cir. 2002) (holding that the border search exception applies at the customs gate at Chicago O'Hare International Airport); United States v. Beras, 183 F.3d 22, 26 (1st Cir. 1999) (holding that the border search exception applied at an airport in Puerto Rico because the traveler was departing on an international flight). *But see, e.g.*, United States v. Mayer, 818 F.2d 725, 727–28 (10th Cir. 1987) (holding that the functional-equivalent-of-border exception did not apply to a domestic airport where there was uncertainty as to whether the plane had come from Mexico).

62. *See* United States v. Flores-Montano, 541 U.S. 149, 152–53 (2004).

63. *See id.* at 153 ("It is axiomatic that the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity."); *Ramsey*, 431 U.S. at 616 ("[S]earches 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.").

64. *See, e.g.*, 8 U.S.C. § 1357(c) (2012) (authorizing warrantless searches at the border by immigration officials); 14 U.S.C. § 89(a) (2012) (permitting warrantless Coast Guard inspections, searches, and seizures on the high seas and in U.S. waters); 19 U.S.C. § 1581(a) (2012) (authorizing customs officers to search any vessel or vehicle anywhere inside the United States, within customs waters, or in any other authorized place without a warrant).

have the right to protect the United States by stopping and examining persons and property entering[65] or leaving[66] the country. The Supreme Court has largely embraced this principle of sovereign prerogative in its Fourth Amendment border search doctrine.[67]

Modern border search cases have typically concerned the smuggling of controlled substances and involved the government applying the border search exception to new situations and emerging technologies.[68] In the Prohibition-era case *Carroll v. United States*,[69] the Court used the border search doctrine as a point of comparison in devising a new exception to the warrant requirement for a nonborder search of automobiles within the country.[70] The *Carroll* Court said that "[t]ravellers may be so stopped [without cause] 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."[71] Domestic automobile searches, in contrast, were held to require probable cause (though not a warrant) because the state does not have the same set of strong national defense interests in the nation's interior that it does at the border, where a search is presumptively reasonable even without probable cause.[72]

The Court echoed *Carroll* over fifty years later in *United States v. Ramsey*[73] and stated that the sovereign has a strong interest in controlling "who and what may enter the country."[74] In *Ramsey*, the Court upheld a statute giving postal inspectors the power to open and inspect packages without a warrant if they had "reasonable cause to suspect" that the package contained contraband.[75] In holding the statute constitutional, the Court stated that the proposition "[t]hat searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining

65. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985) (holding that the government has "plenary authority" to conduct routine warrantless searches "to prevent the introduction of contraband"); *see also Flores-Montano*, 541 U.S. at 152 (holding that the government may search a vehicle crossing the border because of its "interest in preventing the entry of unwanted persons and effects").

66. *See, e.g.*, *Beras*, 183 F.3d at 26 (noting widespread agreement among the circuit courts that the border search exception applies to outgoing as well as incoming travelers).

67. *See, e.g.*, Torres v. Puerto Rico, 442 U.S. 465, 472–73 (1979) ("The authority of the United States to search the baggage of arriving international travelers is based on its inherent sovereign authority to protect its territorial integrity."); *see also* Benjamin J. Rankin, Note, *Restoring Privacy at the Border: Extending the Reasonable Suspicion Standard for Laptop Border Searches*, 43 COLUM. HUM. RTS. L. REV. 301, 306–07 (2011).

68. *See* Sid Nadkarni, *"Let's Have a Look, Shall We?" A Model for Evaluating Suspicionless Border Searches of Portable Electronic Devices*, 61 UCLA L. REV. 146, 184–86 (2013).

69. 267 U.S. 132 (1925).

70. *See id.* at 153–54. The case concerned the smuggling of alcohol during Prohibition. *See id.* at 159–60.

71. *Id.* at 154.

72. *See id.*

73. 431 U.S. 606 (1977).

74. *See id.* at 620.

75. *Id.* at 607–08. The package in question turned out to contain heroin. *Id.* at 610–11.

persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border" required "no extended demonstration."[76]

Under *Ramsey*, officials may conduct routine border searches without a warrant or probable cause when those searches are tethered to the government's interest in examining persons and property seeking entrance to the United States.[77] The Court, however, expressly reserved judgment on 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."[78]

2. Routine and Nonroutine Privacy Intrusions at the Border

Two aspects of the Court's modern border search decisions obscure the clarity of its underlying principles: (1) the reasonableness balancing test, and (2) the distinction between "routine" and "nonroutine" border searches.[79] As weighing individual privacy interests against government intrusions became a more common element of the Court's Fourth Amendment jurisprudence,[80] that balancing test began to crop up in the Court's border search opinions.[81] The Court also stated that an individualized level of suspicion may be necessary for some intrusions beyond the scope of "routine" customs searches and inspections.[82]

There are two broad categories of border searches: "routine" and "nonroutine."[83] A "routine" search of a person and his or her effects crossing an international border into the United States is not subject to any requirement of reasonable suspicion that an item contains contraband or evidence of criminal activity.[84] Border officials can conduct "routine" searches without any individualized suspicion.[85]

On the other hand, a "nonroutine" search involving a high degree of personal intrusion—such as a strip search—requires "reasonable suspicion," which calls for some particularized and objective basis for suspecting

76. *Id.* at 616.
77. *Id.*
78. *Id.* at 618 n.13.
79. THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION § 10.2.1, at 592–93 (3d ed. 2017).
80. *Id.* § 11.3.4, at 706 (describing the rise of the Supreme Court's balancing test for privacy interests in the 1960s).
81. Still, the Court noted that "the Fourth Amendment's balance of reasonableness is qualitatively different at the international border." United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985); *see also Ramsey*, 431 U.S. at 616–19.
82. *See Montoya de Hernandez*, 473 U.S. at 539–41 (upholding a nonroutine, sixteen-hour detention of an individual who was reasonably suspected of smuggling drugs into the country in her alimentary canal); *cf.* United States v. Flores-Montano, 541 U.S. 149, 155 n.3 (2004) (observing that "delays of one to two hours at international borders are to be expected").
83. *Montoya de Hernandez*, 473 U.S. at 541.
84. *Id.* at 537–38.
85. *Flores-Montano*, 541 U.S. at 152 (quoting *Montoya de Hernandez*, 473 U.S. at 538).

wrongdoing.[86] A search crosses the threshold and becomes nonroutine if it is either particularly offensive (such as an intrusive search of the body) or physically destructive.[87] Courts have recognized that nonroutine border searches require a greater level of suspicion than routine searches.[88]

Although the government possesses broad powers to conduct suspicionless border searches and seizures, the Supreme Court and lower courts have generally required at least reasonable suspicion for nonroutine border searches.[89] These invasive searches, which significantly intrude on an individual's Fourth Amendment interests, require a minimal showing of reasonable suspicion.[90] The Supreme Court views the privacy interests implicated by a seizure of an international traveler at the border differently than those involved in the seizure of a person walking the streets of the interior United States.[91] Although the Supreme Court has not explicitly stated what distinguishes a routine from a nonroutine border search, circuit courts have typically examined several factors in making such a determination.[92]

Circuit courts generally agree that the degree of intrusiveness is determinative of the suspicion required to necessitate the search.[93] Lengthy

86. *Montoya de Hernandez*, 473 U.S. at 541–42; *see also* Terry v. Ohio, 392 U.S. 1, 21 (1968) ("And in justifying the particular intrusion the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion.").

87. *See* United States v. Arnold, 533 F.3d 1003, 1007–08 (9th Cir. 2008).

88. *See, e.g.*, United States v. Outlaw, 319 F.3d 701, 703 (5th Cir. 2003) (requiring reasonable individualized suspicion for detentions at immigration checkpoints); United States v. Charleus, 871 F.2d 265, 267–68 (2d Cir. 1989) (requiring reasonable suspicion for nonroutine border searches).

89. *See Montoya de Hernandez*, 473 U.S. at 540–41; Nadkarni, *supra* note 68, at 161–63.

90. *See, e.g.*, United States v. Cotterman, 709 F.3d 952, 966–67 (9th Cir. 2013) (en banc) (requiring reasonable suspicion for a forensic search of a laptop seized at the border).

91. *Compare Terry*, 392 U.S. at 23 ("The crux of this case . . . [is] whether there was justification for [the officer's] invasion of Terry's personal security by searching him for weapons in the course of that investigation."), *with Montoya de Hernandez*, 473 U.S. at 538 ("Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant."), *and* United States v. 12 200-Foot Reels of Super 8mm Film, 413 U.S. 123, 125 (1973) ("Import restrictions and searches of persons or packages at the national borders rest on different considerations and different rules of constitutional law from domestic regulations.").

92. *See* United States v. Braks, 842 F.2d 509, 512 (1st Cir. 1988). The First Circuit considers six factors when determining whether a search is "nonroutine":

> (i) whether the search results in the exposure of intimate body parts or requires the suspect to disrobe;
> (ii) whether physical contact between Customs officials and the suspect occurs during the search;
> (iii) whether force is used to effect the search;
> (iv) whether the type of search exposes the suspect to pain or danger;
> (v) the overall manner in which the search is conducted; and
> (vi) whether the suspect's reasonable expectations of privacy, if any, are abrogated by the search[.]

Id. (footnotes omitted).

93. *See, e.g.*, United States v. Kelly, 302 F.3d 291, 294 (5th Cir. 2002) (stating that "the invasion of the privacy and dignity of the individual" is the "key variable" in determining whether a border search was routine or nonroutine (quoting United States v. Sandler, 644 F.2d

detentions and highly intrusive searches of the person—such as strip searches,[94] extended customs detentions,[95] or body-cavity searches[96]—require some level of particularized suspicion due to their impact on the "dignity and privacy interests of the person being searched."[97] The Supreme Court, however, has never squarely addressed the issue of what level of suspicion these searches require.[98]

The Supreme Court has thus far explicitly limited the routine-nonroutine distinction to those cases involving searches of persons rather than searches of property.[99] In *United States v. Flores-Montano*,[100] 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."[101] Most searches of travelers' luggage, personal effects, and vehicles are found to be sufficiently nonintrusive with regard to individual privacy and dignity interests to qualify as routine border searches that do not require individualized suspicion.[102] When the courts first applied the Fourth Amendment to border searches of computers, they

1163, 1167 (5th Cir. 1981))); Bradley v. United States, 299 F.3d 197, 203–04 (3d Cir. 2002) (holding that the intrusiveness of a border search determines whether that border search was routine or nonroutine); United States v. Tsai, 282 F.3d 690, 694 (9th Cir. 2002) (finding that "the 'degree of intrusiveness'" is "the 'critical factor'" in determining whether a border search is routine (quoting United States v. Molina-Tarazon, 279 F.3d 709, 713 (9th Cir. 2002))); United States v. Johnson, 991 F.2d 1287, 1291 (7th Cir. 1993) (holding that "[r]outine border inspections" do not "embarrass or offend the average traveler").

94. *See, e.g.*, *Bradley*, 299 F.3d at 203–04 (contrasting a routine pat-down with a nonroutine strip search); United States v. Reyes, 821 F.2d 168, 170–71 (2d Cir. 1987) (requiring reasonable suspicion that the defendant was concealing contraband to justify a strip search at the border).

95. *See* United States v. Oyekan, 786 F.2d 832, 836–37 (8th Cir. 1986) (holding that reasonable suspicion justified extended detention for travelers suspected of smuggling drugs).

96. *See, e.g.*, United States v. Handy, 788 F.2d 1419, 1420–21 (9th Cir. 1986) (requiring a "clear indication" that the defendant carried drugs internally to justify a body-cavity search at the border); United States v. Pino, 729 F.2d 1357, 1359 (11th Cir. 1984) (requiring articulable suspicion that a defendant is carrying drugs in his rectal area to justify a cavity search).

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

98. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 541 n.4 (1985) ("[W]e suggest no view on what level of suspicion, if any, is required for nonroutine border searches such as strip, body-cavity, or involuntary x-ray searches.").

99. *See, e.g.*, *Flores-Montano*, 541 U.S. at 152 ("[T]he reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person—dignity and privacy interests of the person being searched—simply do not carry over to vehicles.").

100. 541 U.S. 149 (2004).

101. *Id.* at 152.

102. *See id.* at 154–55 (holding that a search of a vehicle that included disassembly and reassembly of a fuel tank qualified as routine because it did not damage the vehicle and was completed in one hour); Almeida-Sanchez v. United States, 413 U.S. 266, 272 (1973) (holding that the thorough search of a car at the border was not sufficiently intrusive to qualify as nonroutine border search); United States v. Irving, 452 F.3d 110, 123–24 (2d Cir. 2006) (holding that the search of luggage at an airport was not sufficiently intrusive to qualify as a nonroutine search); United States v. Beras, 183 F.3d 22, 26 (1st Cir. 1999) (holding that a pat-down search of a departing international traveler's legs was not sufficiently intrusive to qualify as a nonroutine border search).

held that searches of computers were ordinary searches that did not require suspicion.[103] Searches that physically damage or destroy the property will also be subject to a reasonable suspicion requirement,[104] but the Supreme Court has never held that reasonable suspicion is required for a nondestructive property search at the border.[105]

In the wake of *Flores-Montano*, there is an open question whether the "dignity and privacy interests of the person being searched" ever require limitations on searches of property at the border.[106] The Court's holding that these interests were insufficiently implicated by a vehicle search could be taken as either a conclusion about searches of a specific type of property or as a general statement about all property searches.[107] Unsurprisingly, lower court judges trying to apply *Flores-Montano* to searches of electronic devices have differed on this point.[108]

3. The Scope of Privacy Intrusions in the Digital Context

Electronic devices pose novel challenges for the border search doctrine.[109] With technological advancements, the privacy implications of a rule at one time may be vastly different than the implications of that same rule at a later point in time.[110] If laptops are viewed as simply pieces of property traveling across the border, then the traditional border search doctrine provides little support for requiring any elevated degree of suspicion for their search.[111]

Critics of the traditional border search doctrine argue that searches of laptops or smartphones are analogous to intrusive searches of the body due to the sensitive personal information potentially stored on those devices.[112]

---

103. *See, e.g.*, United States v. Romm, 455 F.3d 990, 997 n.11 (9th Cir. 2006); United States v. Ickes, 393 F.3d 501, 506–08 (4th Cir. 2005).

104. *Flores-Montano*, 541 U.S. at 154 n.2 (distinguishing permissible suspicionless disassembly and reassembly of a fuel tank from "potentially destructive drilling"); *see, e.g.*, United States v. Rivas, 157 F.3d 364, 367–68 (5th Cir. 1998) (holding that drilling into a metal trailer was a nonroutine border search requiring reasonable suspicion); United States v. Robles, 45 F.3d 1, 5–6 (1st Cir. 1995) (holding that drilling into a metal cylinder was a nonroutine search that was justified by the government's reasonable suspicion).

105. *See* Nadkarni, *supra* note 68, at 161–62.

106. *See Flores-Montano*, 541 U.S. at 152.

107. *See id.*; *infra* Part II.

108. *See infra* Part II.

109. *See* Orin S. Kerr, *Every Computer Border Search Requires Case-by-Case Reasonableness, DC Court Holds*, REASON: VOLOKH CONSPIRACY (May 12, 2015, 2:01 AM), https://reason.com/volokh/2015/05/12/every-computer-border-search-r [https://perma.cc/KF4D-3PXQ].

110. *See, e.g.*, Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, *in* SEARCHES AND SEIZURES (THE FOURTH AMENDMENT): ITS CONSTITUTIONAL HISTORY AND THE CONTEMPORARY DEBATE 230, 231 (Cynthia Lee ed., 2011) (describing the declining social importance of public telephones between the 1960s and 2010s).

111. *See, e.g.*, Erick Lucadamo, Note, *Reading Your Mind at the Border: Searching Memorialized Thoughts and Memories on Your Laptop and* United States v. Arnold, 54 VILL. L. REV. 541, 570–71 (2009).

112. *See, e.g.*, Kindal Wright, Comment, *Border Searches in a Modern World: Are Laptops Merely Closed Containers, or Are They Something More?*, 74 J. AIR L. & COM. 701,

"While computers are compact at a physical level, every computer is akin to a vast warehouse of information."[113] A brief search of a smartphone—much less a forensic analysis of the device—reveals intimate data such as a user's personal photos, internet search histories, and email correspondence going back for many years. If the device is connected to the cloud, then the investigator has virtually unlimited access to a person's digital existence.[114] Thus, critics reason that searches of laptops, which may expose a person's innermost thoughts, are as intrusive as strip searches or body-cavity searches that expose the body—searches that courts subject to a reasonable suspicion standard.[115]

This position sits uneasily with longstanding precedent regarding suspicionless searches of nondigital items.[116] Courts have long ruled that border searches of intimate property such as private diaries or personal papers, which almost by definition contain similarly expressive, private materials, require no reasonable suspicion.[117] Some critics therefore charge that computers are no different than any other kind of property carried across the border.[118] A district court outright dismissed the concerns expressed in *Riley* about searching digital technology: "Laptops and cell phones are indeed becoming quantitatively, and perhaps qualitatively, different from other items, but that simply means there is more room to hide digital contraband, and therefore more storage space that must be searched."[119]

Forensic searches of electronic devices can represent distinctly intrusive searches because users are often unaware of what they are carrying on any

---

702 (2009) (concluding that the "proper analogy" for a laptop computer search "should not be that of a closed container, but that of a physical, bodily intrusion due to the large amount of personal memories and personal documents that can be stored on computers").

113. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 542 (2005).

114. A 2018 CBP report noted this concern: "[One] privacy risk concerns CBP's potential over-collection of information from individuals due to the volume of information that is either stored on, or accessible by, today's electronic devices." U.S. DEP'T OF HOMELAND SEC., DHS/CBP/PIA-008(A), PRIVACY IMPACT ASSESSMENT UPDATE FOR CBP BORDER SEARCHES OF ELECTRONIC DEVICES 2 (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/NHD4-RCJT].

115. *See, e.g.*, Nadkarni, *supra* note 68, at 168–69; Rankin, *supra* note 67, at 331.

116. *See supra* Part I.B.1.

117. *See, e.g.*, United States v. Saboonchi, 990 F. Supp. 2d 536, 563 (D. Md. 2014) ("Although it surely is a discomforting concept, there is no principle beyond the shortness of life and the acknowledgement that there is only so much time available to conduct any particular border search that prevents a CBP officer from 'reading a diary line by line looking for mention of criminal activity.'" (quoting United States v. Cotterman, 709 F.3d 952, 962–63 (9th Cir. 2013) (en banc))).

118. One commentator notes that "[a] laptop is simply a new medium through which old ideas, information, habits, and practices are used and recorded." Lucadamo, *supra* note 111, at 571.

119. United States v. Feiten, No. 15-20631, 2016 WL 894452, at *6 (E.D. Mich. Mar. 9, 2016).

given device.[120] Most people understand how to remove items from their suitcase before crossing a border, but few know how to permanently remove unwanted files from a digital device.[121] GPS technology in a vehicle, for example, may store much the same information as a traveler's smartphone without the traveler even realizing it.[122] Electronic devices are capable of storing "a tremendous amount of information that most users do not know about and cannot control."[123] Forensic search software, for example, permits analysts to comb through electronic devices for files "deleted" by the user.[124] This is possible because marking a file "deleted" usually only marks that file cluster as available to be overwritten by other files.[125] Thus, "deleted" files are not instantly removed from the device but may remain on the device undisturbed for an analyst to recover them.[126]

Similarly, the ubiquity of cloud computing potentially places information stored on remote servers in the hands of U.S. border agents.[127] Until 2018, Department of Homeland Security (DHS) agents claimed full authority to search the contents of cloud devices at the border.[128] Border searches gaining access to data in the cloud effectively raid a "virtual safe deposit box," which does not itself cross the border.[129]

The length of time required to undertake a thorough forensic evaluation of an electronic device provides another potential reason to treat searches of these devices as distinct from searches of other forms of property.[130] Electronic devices may be held indefinitely by the government and searched over extended periods of time.[131] Forensic searches of electronic devices are

120. *See generally* SOPHIA COPE ET AL., ELEC. FRONTIER FOUND., DIGITAL PRIVACY AT THE U.S. BORDER: PROTECTING THE DATA ON YOUR DEVICES (2017), https://www.eff.org/wp/digital-privacy-us-border-2017 [https://perma.cc/C6PN-U9Q8].

121. *See id.*; *see also* Matthew B. Kugler, Comment, *The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study*, 81 U. CHI. L. REV. 1165, 1184–85 (2014).

122. *See* George I. Seffers, *DHS Navigates the World of Vehicular Digital Forensics*, AFCEA: SIGNAL (May 25, 2016), https://www.afcea.org/content/Article-dhs-navigates-world-vehicular-digital-forensics [https://perma.cc/TP27-WKTE] (describing DHS searches of in-vehicle systems that "store a vast amount of data, such as recent destinations, favorite locations, call logs, contact lists, text messages, emails, pictures, videos, social media feeds and navigation history").

123. Kerr, *supra* note 113, at 542.

124. *Id.*

125. *Id.*

126. *Id.*

127. *See* Esha Bhandari, *The Government's New Policy on Device Searches at the Border: What You Need to Know*, ACLU (Jan. 9, 2018, 12:45 PM), https://www.aclu.org/blog/privacy-technology/privacy-borders-and-checkpoints/governments-new-policy-device-searches [https://perma.cc/RNJ7-B83Q].

128. *See* U.S. DEP'T OF HOMELAND SEC., *supra* note 114, at 8 (announcing the updated policy that DHS officers may no longer "intentionally use the device to access information that is solely stored remotely").

129. Kugler, *supra* note 121, at 1185.

130. *See, e.g.*, United States v. Saboonchi, 990 F. Supp. 2d 536, 560–61 (D. Md. 2014) (noting the privacy concerns implicated by the "potentially limitless duration and scope of a forensic search").

131. *See* Rankin, *supra* note 67, at 346–47.

typically performed by trained analysts at a government facility away from the border.[132] These searches can last for a period of weeks or even months, during which the travelers have no access to their devices.[133]

C. Searches of Electronic Devices and Data: Riley *and* Carpenter

The case with the greatest impact on the debate surrounding suspicionless border searches of electronic devices is *Riley v. California*,[134] wherein the Supreme Court weighed in on warrantless searches of portable electronic devices incident to arrest.[135] Prior to *Riley*, the Supreme Court had been reluctant to decide Fourth Amendment issues raised by changing privacy expectations with respect to electronic devices.[136] As Chief Justice Roberts noted, "A smart phone of the sort taken from Riley was unheard of ten years ago; a significant majority of American adults now own such phones."[137] In *Riley*, the Supreme Court held that a warrant is required to search a cell phone incident to arrest because of the quantity and quality of information stored on the device.[138] The *Riley* Court concluded that the traditional search-incident-to-arrest exception did not justify dispensing with the warrant requirement for searches of digital devices under the usual concerns for officers' safety or a fear of destruction of evidence.[139]

Riley "marks a turning point in the evolution" of the Court's jurisprudence regarding the Fourth Amendment's application to electronic devices.[140] Chief Justice Roberts, writing for a unanimous Court, commented extensively on individual privacy interests at stake when the government searches portable electronic devices.[141] The Court took care to highlight the "immense storage capacity" of modern cell phones in distinguishing these electronic devices from other forms of personal storage, such as suitcases or trunks.[142] The storage capacity of modern phones—the ability to "store millions of pages of text, thousands of pictures, or hundreds of videos"[143]—means that "a cell phone search would typically expose to the government

132. *See id.* at 320.

133. *See* Kerr, *supra* note 113, at 537–38; *see also, e.g.*, Alasaad v. Nielsen, No. 17-cv-11730-DJC, 2018 WL 2170323, at *21 (D. Mass. May 9, 2018) (noting the confiscation of a traveler's electronic devices for ten months in one instance and fifty-six days in another).

134. 134 S. Ct. 2473 (2014).

135. *See, e.g.*, Miller, *supra* note 13, at 1945.

136. The Court noted that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." City of Ontario v. Quon, 560 U.S. 746, 759 (2010).

137. *Riley*, 134 S. Ct. at 2484.

138. *See id.* at 2485.

139. *Id.* at 2485–88; *see also* Chimel v. California, 395 U.S. 752, 762–63 (1969) (establishing the search-incident-to-arrest exception's principal concerns with officer safety and destruction of evidence).

140. CLANCY, *supra* note 79, § 1.5.2, at 44.

141. *See id.*

142. *Riley*, 134 S. Ct. at 2489.

143. *Id.* at 2478. "Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so." *Id.* at 2489.

far *more* than the most exhaustive search of a house."[144] In distinguishing the Court's new approach to cell phone data searches, Chief Justice Roberts noted "an element of pervasiveness that characterizes cell phones but not physical records."[145] Before the digital age, "people did not typically carry a cache of sensitive personal information with them as they went about their day."[146]

The *Riley* Court also emphasized that data stored on electronic devices is "qualitatively different" than the data found in physical records.[147] The browsing history of an internet-enabled phone "could reveal an individual's private interests or concerns" and, through now-ubiquitous "[h]istoric location information, . . . can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building."[148] *Riley*'s discussion of the privacy implications of cell phone searches echoes the concerns raised by Justice Sotomayor's concurring opinion in *United States v. Jones*,[149] which suggested a revision of another traditional search warrant exception doctrine—the third-party doctrine—in light of advancing cell phone technology.[150]

The *Riley* Court concluded that, given all that modern cell phones "contain and all that they may reveal, they hold for many Americans 'the privacies of life.'"[151] The unanimous Court's "answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant."[152]

In June 2018, in *United States v. Carpenter*,[153] the Supreme Court repeated the privacy concerns expressed in *Riley* regarding cell phone data searches.[154] In *Carpenter*, the Court held that the government's warrantless acquisition of a suspect's cell phone location data in a routine criminal investigation qualified as a search under the Fourth Amendment.[155] Chief

144. *Id.* at 2491 (explaining that a cell phone "also contains a broad array of private information never found in a home in any form—unless the phone is [recovered as part of the search of a home]").

145. *Id.* at 2490.

146. *Id.*

147. *Id.*

148. *Id.*

149. 565 U.S. 400 (2012).

150. *Id.* at 415 (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."); *see also* Elkin Girgenti, *Computer Crimes*, 55 AM. CRIM. L. REV. 911, 941 (2018) (highlighting the influence of Sotomayor's concurring opinion in *Jones* on the majority's opinion in *Riley*).

151. *Riley*, 134 S. Ct. at 2494–95 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

152. *Id.* at 2495.

153. 138 S. Ct. 2206 (2018).

154. David Kris, Carpenter*'s Implications for Foreign Intelligence Surveillance*, LAWFARE (June 24, 2018, 4:51 PM), https://www.lawfareblog.com/carpenters-implications-foreign-intelligence-surveillance [https://perma.cc/S77K-T9SE] ("In its reasoning and result, *Carpenter* strongly resembles the prior decision in *Riley*, which required a warrant for the search incident to an arrest of a cell phone.").

155. *Carpenter*, 138 S. Ct. at 2223.

Justice Roberts's majority opinion cited *Riley* to illustrate a case in which changes in technology have necessitated a more nuanced approach.[156] Responding to Justice Alito's dissenting opinion, the Chief Justice noted that "[w]hen confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents."[157]

With the Supreme Court's unclear application of this case law, the lower courts have reached different conclusions on how to apply this doctrine to border searches of electronic devices.

II. ELECTRONIC PRIVACY AT THE BORDER: A SPLIT IN THE CIRCUIT COURTS

Several circuit courts have heard challenges to evidence obtained during suspicionless border searches following the most recent major border search case in the Supreme Court, *United States v. Flores-Montano*.[158] In 2013, the en banc Ninth Circuit, in *United States v. Cotterman*, anticipated *Riley*'s treatment of heightened privacy concerns triggered by the Fourth Amendment in searches of electronic devices when it ruled that some border searches of digital devices require at least reasonable suspicion.[159] Five years later, the Fourth Circuit, in *United States v. Kolsuz*,[160] explicitly endorsed the same view: that searches of data on electronic devices implicate greater privacy concerns than searches of other physical objects.[161] These decisions, in turn, drew strong criticism from the Eleventh Circuit in *United States v. Touset*,[162] which explicitly rejected *Riley*'s application at the border and reaffirmed the traditional rule that border searches of electronic devices are no different than searches of other physical containers—and thus deserve no special treatment under the Fourth Amendment.[163]

A. Extending Riley *to the Border: The Ninth Circuit in* Cotterman *and the Fourth Circuit in* Kolsuz

Between 2013 and 2018, two circuit courts ruled that the Fourth Amendment required at least reasonable suspicion for some border searches of electronic devices. In 2013, the Ninth Circuit—whose jurisdiction encompasses large portions of the U.S. border with Canada and Mexico and

156. *Id.* at 2214.

157. *Id.* at 2222 ("A search of the information on a cell phone bears little resemblance to the type of brief physical search considered [in prior precedents]." (alteration in original) (quoting *Riley*, 134 S. Ct. at 2485)).

158. *See* Jim Garland & Katharine Goodloe, *Federal Appeals Courts Split on Forensic Searches of Devices Seized at Border*, COVINGTON: INSIDE PRIVACY (May 30, 2018), https://www.insideprivacy.com/international/federal-appeals-courts-split-on-forensic-searches-of-devices-seized-at-border/ [https://perma.cc/SCK4-GGUB]; *see also supra* notes 100–04 and accompanying text (discussing *Flores-Montano*).

159. *See infra* Part II.A.1.

160. 890 F.3d 133 (4th Cir. 2018).

161. *See infra* Part II.A.2.

162. 890 F.3d 1227 (11th Cir. 2018).

163. *See infra* Part II.B.

some of the country's busiest international airports[164]—ruled in *United States v. Cotterman* that a forensic search of an electronic device required some form of reasonable suspicion.[165] Following *Cotterman*, the Fourth Circuit's 2018 decision in *Kolsuz* explicitly applied *Riley*'s understanding of the unique privacy concerns raised by searches of electronic devices to the border.[166]

1. *United States v. Cotterman*

In *Cotterman*, agents seized defendant Howard Cotterman's laptop at the border in response to an alert based, in part, on a past conviction for child molestation.[167] An initial search of the laptop at the border did not reveal incriminating material, but a comprehensive forensic examination of the laptop carried out 170 miles away uncovered child pornography.[168] The lower court granted Cotterman's motion to suppress the evidence found on his laptop,[169] and the Ninth Circuit reversed.[170] In keeping with its longstanding position, the Department of Justice refused to argue that there was reasonable suspicion for the search, which would have preserved the opportunity for the Supreme Court to review whether reasonable suspicion was required for such a search had the Court granted certiorari.[171]

In *Cotterman*, the Ninth Circuit distinguished "a manual review of files on an electronic device" from a forensic "application of computer software to analyze a hard drive."[172] Judge M. Margaret McKeown, writing for the majority, did not explicitly label a forensic search of a laptop "nonroutine," but the opinion makes clear that the "substantial personal privacy interests" impinged by a forensic search moves "beyond the scope of a routine customs search and inspection."[173]

The Ninth Circuit reasoned that a forensic search of a traveler's laptop represented "a thorough and detailed search of the most intimate details of

164. *See Map of the Ninth Circuit*, U.S. CTS. FOR NINTH CIR., http://www.ca9.uscourts.gov/content/view.php?pk_id=0000000135 [https://perma.cc/75AD-UXBU] (last visited Mar. 15, 2019); *see also* U.S. DEP'T OF TRANSP., *supra* note 20, tbl.6.

165. United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013) (en banc).

166. United States v. Kolsuz, 890 F.3d 133, 137 (4th Cir. 2018).

167. *Cotterman*, 709 F.3d at 956.

168. *Id.*

169. *Id.* at 959.

170. *Id.* at 957. The court ultimately concluded that while government agents needed reasonable suspicion of criminal activity to undertake the forensic search of Cotterman's laptop, they met that requirement. *See id.*

171. *See* Orin Kerr, *En Banc Ninth Circuit Holds That Computer Forensic Searches Are like "Virtual Strip Searches" and Require Reasonable Suspicion at the Border*, VOLOKH CONSPIRACY (Mar. 8, 2013, 3:33 PM), http://volokh.com/2013/03/08/en-banc-ninth-circuit-holds-that-computer-forensic-searches-are-like-virtual-strip-searches-and-require-reasonable-suspicion-at-the-border/ [https://perma.cc/UBX4-GH2H]. Ultimately, the Supreme Court denied certiorari and did not hear the case. *See* Cotterman v. United States, 134 S. Ct. 899 (2014).

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

173. *See id.* at 963–64 (quoting United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985)); *see also supra* Part I.B.1.

one's life" and was "a substantial intrusion upon personal privacy and dignity," which required a degree of reasonable suspicion.[174] As such, the court analogized the examination of Cotterman's computer to a strip search and concluded that such a search "intrudes upon privacy and dignity interests to a far greater degree than a cursory search at the border."[175] The court explained that the arduous process involved in the forensic examination, which included copying and searching Cotterman's hard drive in its entirety (including ostensibly deleted files), "is akin to reading a diary line by line looking for mention of criminal activity—plus looking at everything the writer may have erased."[176]

Judge McKeown reasoned that "the uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy and thus renders an exhaustive exploratory search more intrusive than with other forms of property."[177] The court noted that the existence of cloud storage makes searches "even more problematic" since the cloud may offer the government access to sensitive data held on remote servers rather than on the device itself.[178]

The *Cotterman* court believed that the amount of information stored on a computer and the nature of that information justified its rule and observed that "[a] person's digital life ought not be hijacked simply by crossing a border."[179] In dissent, Judge Consuelo Maria Callahan observed, "The majority's opinion turns primarily on the notion that electronic devices deserve special consideration because they are ubiquitous and can store vast quantities of personal information. That idea is fallacious and has no place in the border search context."[180]

2. *United States v. Kolsuz*

United States v. Kolsuz involved a traveler who was found with firearm parts in his luggage and was charged with arms smuggling.[181] After defendant Hamza Kolsuz was detained at Washington Dulles International Airport, customs officers took his phone, manually examined his recent communications, and then transported the device elsewhere for an intensive forensic review.[182] That month-long search, per the court, "yielded an 896-page report that included Kolsuz's personal contact lists, emails, messenger conversations, photographs, videos, calendar, web browsing history, and call logs, along with a history of Kolsuz's physical location down to precise GPS coordinates."[183]

---

174. *Cotterman*, 709 F.3d at 968.
175. *Id.* at 966.
176. *Id.* at 962–63.
177. *Id.* at 966.
178. *Id.* at 965.
179. *Id.*
180. *Id.* at 975 (Callahan, J., dissenting).
181. United States v. Kolsuz, 890 F.3d 133, 136 (4th Cir. 2018).
182. *Id.* at 139.
183. *Id.*

Kolsuz moved to suppress the forensic report, arguing that investigators should have been required to obtain a warrant before the search.[184] After the district court denied the motion and convicted him at trial, relying in part on the report.[185] Kolsuz appealed the denial and argued that his conviction should be overturned either because the border exception did not extend to his case[186] or, in the alternative, because forensic device searches fall within the category of highly intrusive or nonroutine border searches that require greater individualized suspicion than a search of checked luggage would.[187]

Kolsuz argued that the search was unconstitutional because it failed to meet the heightened standards required of especially invasive nonroutine border searches.[188] Writing for the majority, Judge Pamela Ann Harris noted that "border searches of luggage, outer clothing, and personal effects consistently are treated as routine, while searches that are most invasive of privacy—strip searches, alimentary-canal searches, x-rays, and the like—are deemed nonroutine and permitted only with reasonable suspicion."[189] Kolsuz argued that forensic searches are even more invasive than the physical searches the court enumerated, relying on *Riley v. California*'s recognition of the extraordinary volume of personal data that cell phones typically carry.[190]

Judge Harris framed the result in *Kolsuz* as the logical extension of Supreme Court border search precedent in light of the decision in *Riley*.[191] The court noted that Supreme Court border search decisions have held that "individualized suspicion is necessary to justify certain 'highly intrusive searches,' in light of the significance of the individual 'dignity and privacy interests' infringed."[192] The court acknowledged that the Supreme Court "has not delineated precisely what makes a search nonroutine," but it nonetheless concluded—citing *Cotterman*—that "there was a convincing case for categorizing forensic searches of digital devices as nonroutine" even prior to the *Riley* decision.[193]

The Fourth Circuit indicated that *Riley* decisively foreclosed the argument that forensic searches are permissible without reasonable suspicion, noting that "the impact of *Riley* is plain enough that the government's brief does not seriously contest this point."[194] The court observed: "After *Riley*, we think it is clear that a forensic search of a digital phone must be treated as a

184. *Id.* at 139–40. Kolsuz chose not to challenge the manual search of his phone because that search yielded no evidence used against him at trial. *Id.* at 140 n.2.
185. *See id.* at 140–41.
186. *Id.* at 140–42.
187. *See id.* at 142–47. The court quickly dismissed Kolsuz's first argument. *See id.* at 142–44.
188. *See id.* at 144–45.
189. *Id.* at 144.
190. *See id.* at 136–37.
191. *See id.* at 145–47.
192. *Id.* at 144 (quoting United States v. Flores-Montano, 541 U.S. 149, 152 (2004)).
193. *Id.* at 144–45.
194. *Id.* at 146.

nonroutine border search, requiring some form of individualized suspicion."[195]

The *Kolsuz* decision expressly reserved the question of what standard should govern manual device searches that "do not entail the use of external equipment or software" because Kolsuz challenged only the forensic search of his phone, which relied on external implements.[196] Pre-*Riley* Fourth Circuit precedent approved manual device searches without suspicion, as does the Ninth Circuit's decision in *Cotterman*.[197] However, *Riley* seems to undermine this distinction: the case itself involved manual cell phone searches.[198]

B. The Traditionalists Strike Back: The Eleventh Circuit in United States v. Touset

Two weeks after the Fourth Circuit issued its decision in *Kolsuz*, the Eleventh Circuit weighed in on the application of the border search doctrine to electronic devices in *United States v. Touset*. The case arose from the seizure—and subsequent forensic search—of several electronic devices taken from a U.S. traveler at the international airport in Atlanta.[199]

Karl Touset ended up on law enforcement's radar due to a series of payments he made to people in foreign countries who were suspected of distributing child pornography.[200] Upon his return from an international trip, CBP officers inspected Touset's luggage—but the manual search revealed no child pornography.[201] The border officials, however, confiscated two laptops, two external hard drives, and two tablets for further forensic analysis, which revealed child pornography on the laptops and hard drives.[202]

The district court denied Touset's motion to suppress the evidence obtained from the border searches.[203] Touset pled guilty to knowingly transporting child pornography and subsequently appealed the denial of his motion to suppress.[204] On appeal, the government argued that "border agents need no justification whatsoever to detain (in this case for seventeen days)

195. *Id.* But the court recognized that the government nonetheless had reasonable suspicion to conduct a forensic search of Kolsuz's phone. *Id.* at 141.

196. *See id.* at 146 nn.5–6.

197. *See, e.g.*, United States v. Saboonchi, 990 F. Supp. 2d 536, 547–48 (D. Md. 2014) (justifying this two-tiered approach on the theory that manual searches can only invade as much privacy as a law enforcement officer has time to invade, whereas a forensic search can be conducted off-site at the officers' leisure and entails making a lasting copy of the data searched); *see also* Jared Janes, *The Border Search Doctrine in the Digital Age: Implications of* Riley v. California *on Border Law Enforcement's Authority for Warrantless Searches of Electronic Devices*, 35 REV. LITIG. 71, 93–99 (2016).

198. *See* Riley v. California, 134 S. Ct. 2473, 2480–81 (2014); *see also supra* Part I.C.

199. United States v. Touset, 890 F.3d 1227, 1230 (11th Cir. 2018).

200. *Id.*

201. *Id.*

202. *Id.*

203. *See id.* at 1231.

204. *Id.*

and forensically search electronic devices of any American citizen returning from abroad."[205]

Touset followed another Eleventh Circuit case decided earlier in 2018, *United States v. Vergara*,[206] which also concerned the application of the border search exception to a traveler's electronic devices.[207] In *Vergara*, the defendant appealed the denial of his motion to suppress evidence obtained from two cell phones seized by border agents following a cruise to Mexico.[208] The Eleventh Circuit rejected the defendant's argument that these searches required a warrant in the wake of *Riley*.[209] In a brief opinion, Judge William Pryor emphasized that *Riley* "expressly limited its holding to the search-incident-to-arrest exception" and therefore did not impose a warrant requirement for border searches.[210] The defendant conceded that the government had reasonable suspicion for the search, so the *Vergara* court ultimately did not address the question of whether reasonable suspicion was required for the searches.[211]

In *Touset*, the Eleventh Circuit explicitly rejected the reasoning in *Kolsuz* and *Cotterman* in holding that "precedents about border searches of property make clear that no suspicion is necessary to search electronic devices at the border."[212] Judge Pryor, writing for the majority, reaffirmed the Eleventh Circuit's understanding that *Riley* does not apply at the border.[213] The panel therefore remained "unpersuaded" by the routine-nonroutine search distinction highlighted in *Cotterman* and *Kolsuz*.[214]

The *Touset* court emphasized that the Supreme Court rejected the distinction between routine and nonroutine searches of property in *Flores-Montano*.[215] Judge Pryor noted that the Supreme Court "rejected a judicial attempt to distinguish between 'routine' and 'nonroutine' searches" of a vehicle, "as opposed to a more 'intrusive' search of a person."[216] The *Touset* court cited this as decisive support for the argument that any routine-nonroutine distinction has no place in border searches of property: "Property and persons are different."[217] Judge Pryor also pointed out that the only Supreme Court opinion requiring reasonable suspicion for a border search,

205. *Id.* at 1238–39 (Corrigan, J., concurring) (noting that this issue has never been before the Supreme Court). The district court ultimately concluded that the government had reasonable suspicion to conduct the search. *Id.* at 1237 (majority opinion).
206. 884 F.3d 1309 (11th Cir.), *cert. denied*, 139 S. Ct. 70 (2018).
207. *Id.* at 1310–11.
208. *Id.* at 1311.
209. *Id.* at 1312–13.
210. *See id.* at 1312.
211. *See id.* at 1313.
212. United States v. Touset, 890 F.3d 1227, 1229 (11th Cir. 2018).
213. *Id.* at 1234 (citing *Vergara*, 884 F.3d at 1312).
214. *See id.*
215. *See id.* (citing United States v. Flores-Montano, 541 U.S. 149, 152 (2004)).
216. *See id.* at 1233.
217. *See id.* at 1234 (citing *Flores-Montano*, 541 U.S. at 152).

United States v. Montoya de Hernandez,[218] involved the search of a person rather than property.[219]

The Eleventh Circuit noted that its own precedent reflects an unwillingness "to distinguish between different kinds of property."[220] The court ultimately "s[aw] no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property."[221] If, the court reasoned, the Fourth Amendment does not require reasonable suspicion for the search of a crew member's cabin on an incoming international cargo ship—"even though '[a] cabin is a crew member's home,'" which "receives the greatest Fourth Amendment protection"—then it should not require any greater level of suspicion for border searches of electronic devices.[222]

The panel explicitly rejected the notion that the storage capacity of modern electronic devices justified imposing a reasonable suspicion requirement on their searches at the border.[223] Judge Pryor compared a modern electronic device to "a recreational vehicle filled with personal effects or a tractor-trailer loaded with boxes of documents"—neither of which triggers a requirement of reasonable suspicion for a search at the border.[224] The *Touset* court further noted that "[b]order agents bear the same responsibility for preventing the importation of contraband in a traveler's possession regardless of advances in technology."[225]

The Eleventh Circuit found that its traditional standard for measuring a search's intrusiveness on the subject's personal dignity was inapplicable to border searches of property—including electronic devices.[226] The Eleventh Circuit traditionally measures "the 'intrusiveness' of a search of a person's body that requires reasonable suspicion 'in terms of the indignity that will be suffered by the person being searched.'"[227] However, the court found that this exercise is misplaced in searches of electronic devices.[228] "Although it may intrude on the privacy of the owner," the court reasoned, "a forensic search of an electronic device is still a search of property"—and both Supreme Court and Eleventh Circuit precedent require no reasonable suspicion for searches of property at the border.[229]

---

218. 473 U.S. 531 (1985).
219. *See Touset*, 890 F.3d at 1233.
220. *See id.*
221. *Id.*
222. *See id.* (alteration in original) (quoting United States v. Alfaro-Moncada, 607 F.3d 720, 729 (11th Cir. 2010)).
223. *See id.*
224. *Id.*
225. *Id.*
226. *See id.* at 1234 (finding that traditional factors contributing to the personal indignity of the person being searched "are irrelevant to searches of electronic devices").
227. *See id.* (quoting United States v. Vega-Barvo, 729 F.2d 1341, 1345 (11th Cir. 1984)). The Eleventh Circuit analysis focuses on: "(1) physical contact between the searcher and the person searched; (2) exposure of intimate body parts; and (3) use of force." *Id.*
228. *See id.*
229. *Id.*

Moreover, the Eleventh Circuit was particularly unwilling to "create a special rule that will benefit offenders who now conceal contraband in a new kind of property"—in this case, child pornography on portable electronic devices.[230] The court believed that imposing a reasonable suspicion standard would "create special protection for the property most often used to store and disseminate child pornography."[231]

The *Touset* decision, in its explicit rejection of *Riley*'s application at the border and its express disagreement with the reasoning in both *Cotterman* and *Kolsuz*, created a split among the circuit courts as to whether the traditional border search exception properly applies to electronic devices.

III. EVALUATING DIGITAL SEARCHES AT THE BORDER

In light of the divergent approaches to electronic border searches across the Ninth, Fourth, and Eleventh Circuits, this Part argues that the circuit split should be resolved by requiring reasonable suspicion for all border searches of electronic devices. This resolution is consistent with the Ninth and Fourth Circuits' recognition that forensic searches of electronic devices require at least reasonable suspicion.[232] The Supreme Court decisions in *Riley* and *Carpenter* affirm the enhanced Fourth Amendment concerns implicated by searches of digital devices.[233] The spirit of these cases, coupled with an understanding of the nonroutine nature of digital searches, demands that the judiciary rethink the border exception as applied to searches of electronic devices. Moreover, the imposition of a reasonable suspicion requirement for electronic border searches would not adversely impact national security and would fit more squarely with travelers' Fourth Amendment interests.

Part III.A discusses why the Supreme Court's reasoning in *Riley* should carry weight in the context of searches of electronic devices performed at the border. Part III.B argues that all border searches of electronic devices should be considered nonroutine in light of the emphasis in *Riley* and *Carpenter* on the substantial privacy interests that individuals possess in their digital data stored on electronic devices. This Note concludes in Part III.C with a discussion of recent CBP policy changes, which largely endorse the recognition of heightened privacy interests implicated by searches of digital devices.

A. Why Riley *Matters at the Border*

The Supreme Court in *Riley* recognized that searches of electronic devices are distinct from searches of other forms of property and therefore trigger greater Fourth Amendment concerns.[234] The heightened privacy interests implicated by searches of electronic devices—highlighted in *Riley* and

230. *Id.* at 1236.
231. *Id.* at 1235.
232. *See infra* Part III.A.
233. *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018); Riley v. California, 134 S. Ct. 2473, 2494–95 (2014).
234. *See supra* notes 134–52 and accompanying text.

Carpenter—should not go ignored at the border, where nearly every traveler carries an electronic device.[235]

Traditional Fourth Amendment border doctrine balances substantial government interests against the diminished privacy interests of a traveler.[236] The concerns raised in *Riley*[237] should tilt that balance less heavily in favor of the government. The Court in *Riley* held, simply: "Get a warrant."[238] The standard at the border should be: "Get reasonable suspicion."[239]

Traditionalists insist that cell phones or laptops are no different than the letters or ship cabins of old in terms of the government's border search authority—notwithstanding *Riley*'s observation that "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house."[240] This discussion hinges on the question of whether cell phones and laptops are distinct from ordinary "cargo," which does not merit special protection.

Traditionalists argue that the Supreme Court foreclosed this logic with its decision in *Flores-Montano*, which rejected a reasonable suspicion requirement based on intrusiveness for the border search of a vehicle.[241] However, this argument does not properly account for the social and technological changes since that decision was issued in 2004. The Court's opinions in *Riley* and *Carpenter* highlight the immense importance of digital devices in our modern lives.[242] The Eleventh Circuit reasoned in *Touset* that travelers can always leave their devices at home if they want privacy, but *Riley* properly recognized that cell phones are more nearly "an important feature of human anatomy" than they are "just another technological convenience."[243]

Neither the depth of private information accessible on an electronic device nor the traveler's privacy interest in that information disappears at the border. The *Riley* and *Carpenter* decisions took great care to note the strong privacy interests inherent in electronic data—those decisions revisited longstanding exceptions to the warrant requirement in light of advancing technology.[244] To treat border searches of electronic devices as analytically equivalent to the search of a traveler's luggage would be to ignore the unique quality and quantity[245] of the data stored on digital devices.[246] That the data stored on now-ubiquitous electronic devices is virtually impossible for a layperson to

---

235. *See supra* notes 20–22 and accompanying text.
236. *See supra* notes 80–81 and accompanying text.
237. *See supra* notes 134–52 and accompanying text.
238. *See supra* note 152 and accompanying text.
239. *See* Eunice Park, *The Elephant in the Room: What Is a "Nonroutine" Border Search, Anyway? Digital Device Searches Post-*Riley, 44 HASTINGS CONST. L.Q. 277, 306 (2017).
240. Riley v. California, 134 S. Ct. 2473, 2491 (2014). *Compare id.*, *with* United States v. Touset, 890 F.3d 1227, 1235 (11th Cir. 2018).
241. *See supra* notes 101–02 and accompanying text.
242. *See supra* notes 151–57 and accompanying text.
243. *Compare Riley*, 134 S. Ct. at 2484, 2494, *with Touset*, 890 F.3d at 1235.
244. *See supra* notes 140–57 and accompanying text.
245. *See supra* note 138 and accompanying text.
246. *See supra* notes 120–26 and accompanying text.

remove provides even more reason to recognize that an electronic device is a distinct form of property, the search of which calls for individualized suspicion.[247]

B. All Border Searches of Electronic Devices Should Be Considered Nonroutine

The *Riley* Court rejected distinguishing between different levels of a cell phone search.[248] Similarly, courts should not distinguish between routine and nonroutine levels of intrusiveness for a border search of a digital device.

In *Cotterman*, which was decided prior to *Riley*, the Ninth Circuit maintained a distinction between permissibly suspicionless routine manual searches and nonroutine forensic searches that require a greater level of suspicion.[249] The *Kolsuz* court did not reach the question of the justification required for a manual border search of an electronic device, but the narrative thrust of the opinion appears to call for individualized suspicion for all border searches of cell phones.[250]

The fact that a cell phone may be on the person at the time of arrest does not insulate the cell phone from the warrant requirement.[251] The search-incident-to-arrest exception did not justify dispensing with the warrant requirement before officers could search digital data on cell phones under either the traditional concern for the officers' safety or the fear of evidence destruction.[252] Likewise, the fact that a digital device is carried by an international traveler should not exempt the digital device from the protection of a reasonable suspicion requirement.

The circuit split can be resolved and reconciled with *Riley* by establishing that all digital border searches should be categorized as nonroutine—and thus should require reasonable suspicion. This treatment would recognize the unique privacy interests in digital data highlighted in *Riley* and *Carpenter*[253] without substantially upsetting the government's traditional right to secure and protect the border.[254]

C. DHS Agrees: Requiring Reasonable Suspicion for Device Searches Will Not Harm National Security

Mandating reasonable suspicion for digital searches acknowledges travelers' expectation of privacy in digital devices at the border and does not interfere with border agents' ability to do their job. The Department of

247. *See supra* notes 120–26 and accompanying text.
248. *Riley*, 134 S. Ct. at 2492.
249. *See supra* notes 172–76 and accompanying text.
250. *See* United States v. Kolsuz, 890 F.3d 133, 149 (4th Cir. 2018) (Wilkinson, J., concurring) (noting that the majority opinion "may be read by many courts to require individualized suspicion for border searches of all cell phones period"); *see also supra* Part II.A.2.
251. *See supra* notes 137–51 and accompanying text.
252. *See supra* note 139 and accompanying text.
253. *See supra* Part I.C.
254. *See supra* Part I.B.

Homeland Security recognizes this: in January 2018, DHS withdrew a 2009 policy authorizing warrantless, suspicionless searches of electronic devices and replaced it with an updated policy calling for at least reasonable suspicion for some device searches.[255]

The new DHS policy, which cites *Cotterman* among its influences,[256] divides electronic-device searches into two categories: the basic search (manual) and the advanced search (forensic).[257] The 2018 policy requires agents to have reasonable suspicion of "activity in violation of the laws enforced or administered by CBP" or a "national security concern," as well as "supervisory approval," to justify the advanced search.[258] All other searches require no individualized suspicion.[259]

The 2009 CBP policy, which governed border searches of electronic devices at the time of the searches at issue in the cases discussed in this Note,[260] did not distinguish between a basic and advanced search and, in fact, allowed any search to be performed without individualized suspicion.[261] Likewise, the earlier policy permitted confiscation of an electronic device for an on- or off-site search without any level of suspicion.[262]

CBP states that the new policy "will continue to protect the rights of individuals against unreasonable search and seizure and ensure privacy protections while accomplishing its border security and enforcement missions."[263] That the agency adopted a policy requiring reasonable suspicion for certain searches—even though the agency maintains that the law does not require individualized suspicion[264]—amounts to a recognition that a reasonable suspicion policy, for at least forensic border searches of electronic devices, does not pose a substantial national security risk.

Reasonable suspicion imposes a minimal requirement, just the next level up from no suspicion at all.[265] In each of the circuit court cases profiled in Part II, the court found that border agents had reasonable suspicion to conduct searches of the travelers' devices.[266] Border agents rarely undertake lengthy, expensive forensic searches of travelers' digital devices for no particular reason.[267] The agency noted that its agents are professionals and often will

255. *See* U.S. DEP'T OF HOMELAND SEC., *supra* note 114, at 2. The 2018 CBP policy applies to searches performed by CBP officers, not Immigration and Customs Enforcement or Homeland Security Investigations agents. *See* Alasaad v. Nielsen, No. 17-cv-11730-DJC, 2018 WL 2170323, at *3 (D. Mass. May 9, 2018).

256. U.S. DEP'T OF HOMELAND SEC., *supra* note 114, at 2 ("In general, border searches of electronic devices do not require a warrant or suspicion, but certain searches undertaken in the Ninth Circuit must meet a heightened standard.").

257. *Id.* at 5–7.

258. *See id.* at 7.

259. *See id.* at 5–7; *see also Alasaad*, 2018 WL 2170323, at *3–5.

260. *See, e.g.*, *Alasaad*, 2018 WL 2170323, at *5.

261. *See id.*

262. *Id.*

263. *See* U.S. DEP'T OF HOMELAND SEC., *supra* note 114, at 1.

264. *See id.* at 2.

265. *See supra* notes 49–51 and accompanying text.

266. *See supra* notes 170, 195, 205 and accompanying text.

267. *See, e.g.*, U.S. DEP'T OF HOMELAND SEC., *supra* note 114, at 3.

not conduct laptop searches unless facts and circumstances create individualized suspicion—a standard not required by law.[268]

As the *Kolsuz* majority noted: "That the agency has chosen to adopt [the *Cotterman*] requirements, of course, does not establish that they are constitutionally mandated."[269] Travelers deserve to have the reasonable suspicion standard for electronic searches recognized by the judiciary rather than simply accepted as current DHS policy.[270]

CONCLUSION

It seems increasingly likely that the Supreme Court will need to resolve how the border search exception applies to government searches of electronic devices. In the meantime, thousands of travelers' digital devices will be subject to search at the border. The circuit split has significant impact on the millions of travelers—many of whom travel with confidential or highly sensitive business information—that pass through the U.S. borders each year and the agents responsible for protecting those borders. Minimal harm will result from imposing a reasonable suspicion requirement for border searches of electronic devices. Calling for reasonable suspicion for border searches of electronic devices properly recognizes both *Riley*'s Fourth Amendment concerns regarding digital searches and the longstanding right of a sovereign nation to protect its borders.

268. *See id.* at 2.

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

270. *See* Riley v. California, 134 S. Ct. 2473, 2491 (2014) ("[T]he Founders did not fight a revolution to gain the right to government agency protocols.").