University of Cincinnati Law Review

Volume 88 | Issue 1 Article 6

October 2019

A Constitutional Limbo: Searches of Electronic Devices at the International Border

Michael Soder
University of Cincinnati, soderml@mail.uc.edu

A CONSTITUTIONAL LIMBO: SEARCHES OF ELECTRONIC DEVICES AT THE INTERNATIONAL BORDER

Michael Soder

I. INTRODUCTION

Searches of travelers and their personal effects at the international border are far from a new phenomenon.[1] Individuals, whether they travel internationally or not, are likely aware of the in-depth security process for crossing the border.[2] The Supreme Court has recognized that under the "border search" exception, warrantless searches of persons and property are reasonable, and therefore allowed, simply because they occur at the border.[3] As a result, customs officials have plenary authority to search a traveler's property when said traveler is entering or exiting the country.[4] In the digital age, however, searches of cell phones, laptops, cameras, and other electronic devices at the border have become an increasingly contentious, and common, issue.[5] Scholars[6] and courts[7] have increasingly recognized the need to determine the proper constitutional treatment for searches of electronic devices at the border.

United States Customs and Border Protection ("CBP") recently reported that "[i]n this digital age, border searches of electronic devices are essential to enforcing the law at the U.S. border and to protecting the American people."[8] This stance is represented through both CBP's and

1. *See* Boyd v. United States, 116 U.S. 616 (1886).

2. *See* TRANSP. SEC. ADMIN., *Security Screening*, https://www.tsa.gov/travel/security-screening.

3. *See* United States v. Ramsey, 431 U.S. 606, 616 (1977).

4. *See infra* Section II-C.

5. *See, e.g.,* United States v. Touset, 890 F.3d 1227 (11th Cir. 2018); United States v. Kolsuz, 890 F.3d 133 (4th Cir. 2018); *Examining Warrantless Smartphone Searches at the Border: Hearing on S. 2462 Before the S. Subcomm. on Fed. Spending Oversight and Emergency Mgmt.,* 115TH Cong. 1 (2018), https://www.hsgac.senate.gov/subcommittees/fso/hearings/examining-warrantless-smartphone-searches-at-the-border.

6. *See, e.g.,* Laura K. Donohue, *Electronic Search and Seizure at the Border,* 128 YALE L.J.F. (forthcoming); Thomas Miller, Note, *Digital Border Searches After Riley v. California*, 90 WASH. L. REV. 1943 (2015); Matthew B. Kugler, Comment, *The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study*, 81 U. CHI. L. REV. 1165, 1211 (2014); Louisa K. Marion, *Borderline Privacy: Electronic Border Searches After Cotterman*, 28-SUM CRIM. JUST. 36 (SUMMER 2013).

7. *See, e.g.,* Alasaad v. Nielsen*,* No. 17-CV-11730-DJC, 2018 WL 2170323 (D. Mass. May 9, 2018); *Touset*, 890 F.3d 1227; *Kolsuz*, 890 F.3d 133; United States v. Vergara*,* 884 F.3d 1309 (11th Cir. 2018); United States v. Caballero, 178 F. Supp. 3d 1008 (S.D. Cal. 2016); United States v. Ramos, 190 F. Supp. 3d 992 (S.D. Cal. 2016); United States v. Cotterman, 709 F.3d at 952 (9th Cir. 2013) (en banc); United States v. Saboonchi, 990 F. Supp. 2d 536 (D. Md. 2014).

8. U.S. CUSTOMS & BORDER PROT., *CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics* (Jan. 5, 2018) (quoting John Wagner), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and.

the United States Immigration and Customs Enforcement's ("ICE") policy directives authorizing digital border searches.[9] In 2016, CBP conducted 19,051 border searches of electronic devices.[10] In 2017, this number increased to 30,200 searches.[11] Likewise, in 2015, ICE reported searching 4,444 cell phones and 320 other electronic devices; in 2016, the number of digital device searches increased to 23,000.[12] Such a sharp rise in the number of searches conducted is cause for alarm.[13] Given that these searches reveal a wealth of information, ranging from emails, text messages, and photographs, from 2011 to 2017 international travelers filed approximately 250 complaints with the Department of Homeland Security.[14]

The Supreme Court has yet to determine what the Fourth Amendment requires regarding digital searches at the border, leaving lower federal courts to handle this difficult task. However, lower courts are not completely without guidance. In three Supreme Court cases—*United States v. Ramsey*,[15] *United States v. Montoya de Hernandez*,[16] and *United States v. Flores-Montano*[17]—a distinction between "routine" and "nonroutine" border searches emerged. Based on this distinction, some lower courts began to require some level of suspicion for forensic searches of electronic devices at the border, notwithstanding the traditional border search exception.[18]

---

9. *See* U.S. CUSTOMS & BORDER PROT., *Border Search of Electronic Devices, CBP Directive No. 3340-049A* (Jan. 4, 2018), https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf; *see also* U.S. IMMIGRATION & CUSTOMS ENF'T, *Border Searches of Electronic Devices, ICE Directive No. 7-6.1* (August 18, 2009, reviewed August 18, 2012).

10. U.S. CUSTOMS & BORDER PROT., *supra* note 8.

11. *Id.*

12. *Examining Warrantless Smartphone Searches at the Border: Hearing on S. 2462 Before the S. Subcomm. on Fed. Spending Oversight and Emergency Mgmt.,* 115TH Cong. 1 (testimony of Laura K. Donohue, Professor of Law, Georgetown University Law Center) (citing *Daniel* Victor, *What Are Your Rights if Border Agents Want to Search Your Phone?*, N.Y. Times (Feb. 14, 2017), https://www.nytimes.com/2017/02/14/business/border-enforcement-airport-phones.html).

13. CBP officials reported that these searches affected less than 1% of the approximate 300 million travelers who arrived in the United States in 2017. Ron Nixon, *Cellphone and Computer Searches at U.S. Border Rise Under Trump*, NEW YORK TIMES (Jan. 5, 2018), https://www.nytimes.com/2018/01/05/us/politics/trump-border-search-cellphone-computer.html. Although this is a notably small percentage, this does not change the fact that thousands of travelers have their private personal information revealed during these searches.

14. *See* Charlie Savage and Ron Nixon, *Privacy Complaints Mount Over Phone Searches at U.S. Border Since 2011*, NEW YORK TIMES (Dec. 22, 2017), https://www.nytimes.com/2017/12/22/us/politics/us-border-privacy-phone-searches.html. Travelers whose electronic devices were searched described themselves as being "made to feel like a criminal" and experiencing a "blatant abuse of privacy." *Id.*

15. 431 U.S. 606 (1977).

16. 473 U.S. 531 (1985).

17. 541 U.S. 149 (2004).

18. *See* United States v. Saboonchi, 990 F. Supp. 2d 536, 569 (D. Md. 2014); *see also* United

To complicate the matter, in 2014 the Supreme Court announced in *Riley v. California* that generally, a cell phone cannot be seized incident to a lawful arrest without a warrant supported by probable cause.[19] After 2014, a small minority of lower courts recognized *Riley*'s reasoning as supporting a constitutional requirement of reasonable suspicion to search a traveler's electronic device at the border.[20] Most recently, in May 2018, two Federal Circuit Courts reached opposing conclusions on the issue, offering both new perspectives and preserving the challenge of how "suspicionless" digital device searches should be treated. The Fourth Circuit, in *United States v. Kolsuz*, relied in part on *Riley* to conclude that the Fourth Amendment requires some form of "individualized suspicion" to forensically search electronic devices at the border.[21] In contrast, the Eleventh Circuit, in *United States v. Touset*, rejected an application of *Riley*, and upheld "suspicionless" forensic searches of an electronic device.[22]

In light of the recent decisions of *Kolsuz* and *Touset,* this Article will explore the constitutionality of searches of electronic devices at the international border, and suggest that the Fourth Amendment requires reasonable suspicion to conduct such searches. Although the Article mainly considers the constitutionality of forensic searches, the reasoning applies equally as forcefully to manual searches. First, Section II explores the relevant doctrinal foundation for the border search exception, discussing general Fourth Amendment standards, the impact of technology in defining the "reasonableness" of searches, and the border search exception more generally. Section III narrows the focus to a discussion of the intersection of technology and the border search exception and differing approaches taken by federal circuit courts regarding searches of electronic devices. Lastly, Section IV analyzes the differing approaches to determine the appropriate Fourth Amendment analysis of searches of electronic devices at the border. The following

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

19. 573 U.S. 373, 401 (2014).

20. *See, e.g.,* United States v. Kolsuz, 890 F.3d 133, 137 (4th Cir. 2018). Even before *Riley*, a few lower courts began requiring reasonable suspicion for forensic searches of electronic devices. *See Cotterman*, 709 F.3d at 968; *see also Saboonchi*, 990 F. Supp. 2d at 569. In 2017, the American Civil Liberties Union filed a lawsuit on behalf of 10 plaintiffs against the Department of Homeland Security ("DHS"), challenging the practice of warrantless digital device searches under the Fourth Amendment. The federal district court denied the DHS's motion to dismiss, finding that *Riley* is at least partially applicable in the border search context. *See* Alasaad v. Nielsen, Co. 17-CV-11730-DJC, 2018 WL 2170323, at *21 (D. Mass. May 9, 2018). Plaintiffs' also alleged that the practice violated their First Amendment rights by burdening their "protected rights of freedom of speech and association and chill[ing] the exercise of these rights." *Id.* at *22. Likewise, the court rejected DHS's motion to dismiss this claim. *Id.* at *24.

21. *Kolsuz*, 890 F.3d at 144.

22. United States v. Touset, 890 F.3d at 1234-35 (11th Cir. 2018).

analysis suggests that the Fourth Circuit is correct and, furthermore, that the Fourth Amendment requires reasonable suspicion for all searches of electronic devices at the border.

II. BACKGROUND

The following section proceeds in three parts, providing an overview of the jurisprudence underlying the split between the Fourth and Eleventh Circuits. Part A introduces the Fourth Amendment, explaining the coverage and requirements of the Fourth Amendment. Part B then explores how courts have interpreted the Fourth Amendment in light of technological advances, particularly electronic devices, such as cell phones. Finally, Part C focuses on the border search exception to the Fourth Amendment, and the determination of what constitutes a reasonable search and seizure at the international border.

A. Fourth Amendment Standards

The Fourth Amendment to the United States Constitution provides:

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[23]

The basic aim of this Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."[24] From a historical standpoint, the Fourth Amendment represents the Framers' response to "the reviled 'general warrants' and 'writs of assistance'" that existed under British rule, which allowed "British officers to rummage through homes in an unrestrained search for evidence of criminal activity."[25] The Supreme Court subsequently imposed further limitations and restraints on the government's search and seizure power via adoption of the exclusionary rule.[26] This rule, serving as a deterrent function, generally prohibits the prosecution from presenting evidence obtained in violation of a defendant's Fourth Amendment rights.[27]

---

23. U.S. Const. amend. IV.

24. Carpenter v. United States, 138 S.Ct. 2206, 2213 (2018) (quoting Camara v. Mun. Court of City and Cty. of San Francisco, 387 U.S. 523, 528 (1967)).

25. *Riley v. California,* 573 U.S. 373, 403 (2014).

26. *See* Weeks v. United States, 232 U.S. 383, 392 (1914) ("to obtain conviction by means of unlawful seizures . . . should find no sanction in the judgments of the courts . . . .").

27. *See* Davis v. United States, 564 U.S. 229, 231-32 (2011); *see also* Elkins v. United States, 364

Although judicial interpretation of both the meaning and coverage of the Fourth Amendment has dramatically changed over the years,[28] a court's approach to analyzing a search can be distilled down into two inquiries.[29] First, the Amendment is only applicable if the incident at question is deemed a "search,"[30] which turns on whether government agents invade a person's individual interest that is "constitutionally protected" by the Amendment.[31] To determine if an interest is constitutionally protected—and thus whether there has been a search—courts generally apply the mystical-sounding "reasonable expectation of privacy" test to determine whether a particular search is intrusive enough to implicate the Fourth Amendment.[32] A reasonable expectation of privacy exists if (1) an individual has an actual expectation of privacy in an object or place and (2) society is prepared to recognize that expectation as reasonable.[33]

The second requirement imposed by the Amendment is that the search itself must be reasonable, as "the ultimate touchstone of the Fourth

U.S. 206, 217 (1960) (the rule's purpose is "to compel respect for the constitutional guaranty [of the Fourth Amendment] . . . .") The Court has also held that the exclusionary rule also applies to state courts, via the Fourteenth Amendment. Mapp v. Ohio, 367 U.S. 643, 655 (1961). However, as the exclusionary rule is based on a deterrence effect, the Supreme Court has progressively narrowed the rule's application through several exceptions. *See, e.g,* United States v. Leon, 468 U.S. 897, 913 (1984) (good-faith exception); Murray v. United States, 487 U.S. 533, 537 (1988) (independent source doctrine); Nix v. Williams, 467 U.S. 431 (1984) (inevitable discovery doctrine); Wong Sun v. United States, 371 U.S. 471 (1963) (attenuation/dissipation of taint doctrine).

28. *See* WILLIAM E. RINGEL, SEARCHES AND SEIZURES ARRESTS AND CONFESSIONS §1.1 (2D ED. 2018).

29. 68 AM. JUR. 2D SEARCHES AND SEIZURES §12 (2D 2018).

30. *See* 1 WAYNE R. LAFAVE, SEARCH & SEIZURE §2:1 (5TH ED. 2018) ("[c]entral to an understanding of the Fourth Amendment . . . is a perception of what police activities, under what circumstances and infringing upon what areas and interests, constitute . . . a search . . . within the meaning of that Amendment.").

31. RINGEL, SEARCHES AND SEIZURES ARRESTS AND CONFESSIONS §2:1; *see* Katz v. United States, 389 U.S. 347, 350 (1967) ("the Fourth Amendment cannot be translated into a general constitutional 'right to privacy.'").

32. *See Katz*, 389 U.S. at 361 (1967) (Harlan, J., concurring); *see also* Smith v. Maryland, 442 U.S. 735, 740 (1979) ("Consistently with *Katz*, this Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by the government action.") (internal citations omitted). *Katz* represented a shift from then existing Fourth Amendment jurisprudence, which relied exclusively on a property-rights, trespass interpretation of the Amendment. *See* Boyd v. United States, 116 U.S. at 627 (1886) ("every invasion of private property, be it ever so minute, is a trespass.") (quoting Entick v. Carrington, 19 Howell St. Tr. 1029, 1066 (1765) (Eng.)). However, the Court subsequently clarified that *Katz* did not abrogate the property-rights interpretation. *See* United States v. Jones, 565 U.S. 400, 409 (2011) ("the *Katz* reasonable-expectation-of-privacy test has been *added to, not substituted for*, the common-law trespassory test.") (emphasis in original).

33. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring). Generally, the permissibility or reasonableness of a particular search will turn on the balance between an individual's Fourth Amendment interests against promoting legitimate governmental interests. *See* 68 AM. JUR. 2D SEARCHES AND SEIZURES §12 (2D 2018).

Amendment is reasonableness."[34] Generally, this requires officers or government agents to obtain a judicial warrant from a "neutral and detached magistrate," as opposed to "being judged by the officer engaged in the often competitive enterprise of ferreting out crime."[35] This requirement of judicial oversight provides both an "orderly procedure" and the impartiality needed to realize the guarantees of the Fourth Amendment.[36] A warrant must be based upon a finding of probable cause—a "fluid concept" that turns on "particular factual context," and is thus a "practical, nontechnical conception."[37] Given this standard, probable cause requires "specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion."[38] Put another way, probable cause exists when "the facts available to . . . [an officer] would warrant a person of reasonable caution in the belief that contraband or evidence of a crime is present."[39] Although courts have traditionally treated warrantless searches as *per se* unreasonable under the Fourth Amendment, there are a few "specially established and well-delineated exceptions" to the warrant requirement.[40]

However, even if a particular search falls within an exception to the warrant requirement, courts can still require some type of justification for the search, such as probable cause[41] or reasonable suspicion.[42] Reasonable suspicion requires more than "a mere hunch," but the "level of suspicion . . . is considerably less than proof of wrongdoing by a preponderance of the evidence and obviously less than is necessary for probable cause."[43]

34. Riley v. California, 573 U.S. 373, 381 (2014) (internal citation omitted).

35. Johnson v. United States, 333 U.S. 10, 14 (1948) ("When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or Government enforcement agent.").

36. *See* United States v. Jeffers*,* 342 U.S. 48, 51 (1951) (internal citation omitted); *see also* Illinois v. Gates, 462 U.S. 213, 236 (1983) ("the possession of a warrant . . . greatly reduces the perception of unlawful or intrusive police conduct, by assuring 'the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search.'") (quoting United States v. Chadwick, 433 U.S. 1, 9 (1977)); *see also* Beck v. Ohio, 379 U.S. 89, 96 (1964) ("An arrest without a warrant bypasses the safeguards provided by an objective predetermination of probable cause[.]").

37. *Gates*, 462 U.S. at 231-32; Brinegar v. United States, 338 U.S. 160, 176 (1949).

38. Terry v. Ohio, 392 U.S. 1, 21 (1968).

39. Florida v. Harris, 568 U.S. 237, 243 (2013) (internal citations and quotations omitted).

40. Katz v. Unites States, 389 U.S. 347, 357 (1967); *see, e.g.,* Carroll v. United States, 267 U.S. 132, 153-56 (1925); Cooper v. State of California, 386 U.S. 58 (1967); Warden Md. Penitentiary v. Hayden, 387 U.S. 294, 298-300 (1967). Typical exceptions include searches of automobiles, Collins v. Virginia, 138 S.Ct. 1663, 1669 (2018), and searches incident to arrest, Riley v. California, 573 U.S. 373, 382-85 (2014).

41. *See* Chambers v. Maroney, 399 U.S. 42, 51 (1970).

42. *See Terry*, 392 U.S. 1, 36-37. A search only requiring reasonable suspicion, like one requiring probable cause, is still based on the totality of the circumstances approach. *See* United States v. Cortez, 449 U.S. 411, 417 (1981).

43. Navarette v. California, 572 U.S. 393, 397 (2014) (internal citations and quotations omitted).

In essence, an officer or governmental agent must have "a particularized and objective basis for suspecting the particular person stopped of criminal activity."[44] This standard is satisfied when a government agent can identify "specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion."[45]

B. The Fourth Amendment in the Digital Age[46]

Given the seemingly exponential technological advances within the past half-century, courts have struggled to interpret the Fourth Amendment in light of these developments.[47] The intersection of technological advances and the Fourth Amendment have created a difficult setting for judicial determination of "reasonable" searches.[48]This is particularly so given the Fourth Amendment's historical tie to real property concepts.[49] Yet, as technology has indeed "propelled us into a new era,"[50] "the facts that the Fourth Amendment regulates . . . are constantly evolving" due to the new tools afforded to officers and government agents, as well as the advent of technological devices available to the general population.[51] More often than not, new technologies have "destabilized the relationship" between privacy and property.[52]

The struggle to apply the Fourth Amendment within this context largely results from the application of *Katz v. United States*'s reasonable expectation of privacy test.[53] Although *Katz* did arguably expand the

44. *Id.* at 404 (internal citations omitted).

45. *Terry*, 392 U.S. at 21.

46. For an insightful and in-depth overview, *see* Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553 (2017).

47. *See, e.g.,* Katz v. United States, 389 U.S. 347 (1967) (electronic listening and recording device used to hear a conversation in a public phone booth); Kyllo v. United States, 533 U.S. 27 (2001) (use of thermal imager to detect infrared radiation emanating from a home); United States v. Jones, 565 U.S. 400 (2011) (installation of Global-Positioning-System on Defendant's vehicle); Riley v. California, 573 U.S. 373 (2014) (search of Defendant's cellphone incident to arrest).

48. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 808 (2004) ("no one knows whether an expectation of privacy in a new technology is 'reasonable.'").

49. *Id.* at. 809. Early Fourth Amendment jurisprudence established that the Framer's considered common law trespass as "sufficiently explanatory of what was meant by unreasonable searches and seizures." *See* Boyd v. United States, 116 U.S. 616, 626-27 (1886).

50. Donohue, *supra* note 46 at 554.

51. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 485 (2011).

52. Kerr, *supra* note 48 at 827.

53. *See, e.g.,* Michael Abramowicz, *Constitutional Circularity*, 49 UCLA L. REV. 1, 60-61 (2001) ("Fourth Amendment doctrine, moreover, is circular, for someone can have a reasonable expectation of privacy in an area if and only if the Court has held that a search in that area would be unreasonable."); Kerr, *supra* note 48 at 808.

coverage of the Fourth Amendment,[54] there is no "talisman that determines in all cases" which privacy expectations are reasonable; courts must examine the particular search to determine if the search was constitutionally permissible.[55]

Even with these difficulties, Fourth Amendment protections have been established based on privacy concerns stemming from technological advances.[56] In *Riley v. California*, the Court considered whether police, without a warrant, could search digital information on a cell phone that was seized incident to an arrest.[57] Prior precedent established a categorical rule allowing the warrantless search of an individual incident to a lawful arrest,[58] but the Court rejected a mechanical interpretation of precedent.[59] Instead, the Court assessed the balance of "the degree to which . . . [the search] intrudes upon an individual's privacy" versus the need of the search for promoting "legitimate governmental interests."[60] Regarding the governmental interests, the Court noted that the justifications underlying the search incident to arrest doctrine, destruction of evidence and harm to officers, would not be served in applying the exception to searches of cell phones.[61] Although an arrestee does have a diminished privacy interest, Chief Justice Roberts engaged in an in-depth analysis of one's privacy interest in a cell phone.[62]

The Court distinguished searches of cell phones from searches of physical items, as cell phones "differ in both a quantitative and qualitative

54. *See* 1 LAFAVE, SEARCH & SEIZURE §2.1(B).

55. O'Connor v. Ortega, 480 U.S. 709, 715 (1987). Some scholars have posited that determining the scope of the Fourth Amendment inherently entails "value judgments" by the courts. *See, e.g.,* Michael R. Gardner*, Rediscovering Trespass: Towards a Regulatory Approach to Defining Fourth Amendment Scope in a World of Advancing Technology*, 62 BUFF. L. REV. 1027, 1069 (2014).

56. *See, e.g.,* Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that Thermovision imaging of a house is an unlawful search); Riley v. California, 573 U.S. 373 (2014).

57. *Riley*, 573 U.S. at 378. The case consolidated two separate appeals. In the first case police seized the defendant's "smart phone" and examined it both on the spot and later at the police station. *Id.* at 379-80. In the second case, police seized defendant's "flip phone," accessed the recent call log, and used that information to ascertain an address and subsequent search warrant. *Id.* at 380-81.

58. *Id.* at 382-84 (citing Chimel v. California, 395 U.S. 752, 762-63 (1969) (allowing a search of "the arrestee's person and the area within his immediate control") (internal quotations and citations omitted)); *see* United States v. Robinson, 414 U.S. 218, 235 (1973) (rejecting a case-by-case adjudication to determine the constitutionality of a search of a person incident to a lawful custodial arrest); *see also* United States v. Chadwick, 433 U.S. 1, 15 (1977) (limiting the exception to "personal property immediately associated with the person of the arrestee.").

59. *Riley*, 573 U.S. at 386.

60. *Id.* at 385 (citing Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

61. *Riley*, 573 U.S. at 386-89. An officer could simply seize the phone and thus eliminate either risk.

62. *Id.* at 392 (when "privacy-related concerns are weighty enough" a "search may require a warrant, notwithstanding the diminished expectations of privacy of the arrestee.") (quoting Maryland v. King, 569 U.S. 435, 463 (2013)).

sense from other objects" that might be on an arrestee's person.[63] The immense storage capacity of cell phones, the Court articulated, creates a "substantial additional intrusion on privacy" as opposed to a simple search of more traditional physical items.[64] Moreover, modern cell phones hold "the privacies of life,"[65] and the conglomeration of types of information stored in a cell phone allows for the sum of an individual's private life to be reconstructed through one search.[66] Given the privacy concerns implicated through search of a cell phone, the Court held that a warrant is generally required to search a cell phone, even when the cell phone is seized incident to arrest.[67]

C. The Border Search Exception[68]

The "border-search doctrine" is a "narrowly defined"[69] and "historically recognized" exception to the Fourth Amendment's warrant requirement, establishing that searches conducted at the border without a warrant or probable cause are nonetheless reasonable.[70] The exception stems from two, interrelated lines of reasoning that led the Supreme Court

63. *Riley*, 573 U.S. at 393 (analogizing a search of a cell phone to a search of physical items "is like saying a ride on horseback is materially indistinguishable from a flight to the moon.").

64. *Id.*

65. *Id.* at 403 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

66. *Riley,* 573 U.S. at 394-97 (The Court also noted a cell phone's "element of pervasiveness" as nearly every individual carries one on their person at any given time).

67. *Id.* at 401. In 2018, the Supreme Court addressed in *Carpenter v. United States* how the Fourth Amendment applies to "the ability to chronicle a person's past movements through the record of his cell phone signals." 138 S.Ct. 2206, 2216 (2018). The police had obtained the Defendant's location through the use of cell-site location information collected by wireless carriers via cellular signal tapping into local cell sites. *Id.* at 2211-12. The majority declined to extend *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976), to "cover these novel circumstances." *Id.* at 2216-17. The Court went on to hold that the government's actions invaded the defendant's "reasonable expectation of privacy in the whole of his physical movements," and thus violated the Fourth Amendment. *Id.* at 2219.

68. Since the exception applies to the border, it covers individuals and property that are both entering and exiting the country. *See, e.g.,* United States v. Oriakhi, 57 F.3d 1290, 1296-97 (4th Cir. 1995); United States v. Roberts, 274 F.3d 1007 (5th Cir. 2001). Searches need not occur at the physical border as the exception covers searches at the "functional equivalent of a border," such as airports. *See e.g.,* Almeida-Sanchez v. United States, 413 U.S. 266, 272-73 (1973). Additionally, extended border searches, which occur after the travelers "actually entry has been effected," are encompassed within the exception. *See, e.g.,* United States v. Guzman-Padilla, 573 F.3d 865, 883 (9th Cir. 2009) (requiring reasonable suspicion for extended border searches as these searches "intrude more on an individual's normal expectations of privacy[.]").

69. *See* United States v. Pickett, 598 F.3d 231, 234 (5th Cir. 2010) (citing United States v. Ramsey, 431 U.S. 606, 619 (1977)).

70. *See Ramsey*, 431 U.S. at 619. The border search exception is not based on the "exigent circumstances" doctrine, but rather is a "historically recognized exception to the Fourth Amendment's" warrant requirement, dating back to *Boyd* and *Carroll*. *Id.* at 617, 621 (citing *Boyd*, 116 U.S. at 623; Carroll v. United States, 267 U.S. 132 (1925)).

to subject border searches to less constitutional constraints.[71] First, in *Ramsey* the Supreme Court noted that the First Congress viewed customs searches at the border as routinely accepted.[72] Second, searches at the border evoke heightened governmental interests, such as concerns of sovereignty, territorial integrity, and Congress's plenary power to regulate the border.[73] Given these weighty considerations, the Court has drawn a sharp distinction between border and domestic searches:[74]

> Travelers may so be stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in. But those lawfully within the country . . . have a right to free passage without interruption or search unless there is . . . probable cause for believing that their vehicles are carrying contraband or illegal merchandise.[75]

Thus, searches at the border are "reasonable simply by virtue of the fact that they occur at the border,"[76] and as a result, an individual's expectation of privacy is less at the border compared to the interior of the country.[77]

---

71. *See Ramsey*, 431 U.S. at 616.

72. *See id.* at 616-17 (citing *Boyd,* 116 U.S. at 623); *see also* Act of July 31, 1789, ch. 5, §24, 1 Stat. 29, 43 (1789) (allowing customs officials to search, without a warrant, vessel or cargo suspected of illegally entering the United States). Reflecting on this statute, the Court commented, "it is clear that the members of [the First Congress] did not regard searches and seizures of this kind as 'unreasonable,' and they are not embraced within the prohibition of the [Fourth Amendment]." *Ramsey*, 431 U.S. at 617 (quoting *Boyd*, 116 U.S. at 623).

73. Torres v. Com. of 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."); U.S. Const. art. I, §8, cl. 1 ("[t]o lay and collect Taxes, Duties, Imposts and Excises"); *Id.* art. I, §8, cl. 3 ("[t]o regulate Commerce with foreign Nations); *Id.* art. I, §8, cl. 4 ("[t]o establish a[] uniform Rule of Naturalization").

74. *See* 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.").

75. *Carroll*, 267 U.S. at 154.

76. United States v. Flores-Montano, 541 U.S. 149, 152-53 (2004) (quoting *Ramsey*, 431 U.S. at 616)).

77. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 538-39 (1985) ("the Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior.") (internal citations omitted); *see also* United States v. Alfaro-Moncada*,* 607 F.3d 720, 732 (11th Cir. 2010); United States v. Hidalgo-Gato, 703 F.2d 1267, 1271 (11th Cir. 1983) ("On crossing a border the individual is on notice that a search may be made[.]") (quoting United States v. Stanley, 545 F.2d 661, 667 (9th Cir. 1979)); United States v. Ickes, 393 F.3d 501, 506 (4th Cir. 2005) ("When someone approaches a border, he should not be surprised that customs officers characteristically inspect luggage . . . it is an old practice and is intimately associated with excluding illegal articles from the country") (internal citations and quotations omitted). Scholars have noted two factors justifying this reduced expectation of privacy: (1) travelers crossing the border are on notice that searches are likely to be made, and (2) searches are made to the class of travelers as a whole and not to "individual[s] singled out for a search."; 5 WAYNE R. LAFAVE, SEARCHES & SEIZURES §10.5(A) (5TH ED. 2018) (citing *Border Searches and the Fourth Amendment*, 77 YALE L. J. 1007, 1012 (1968)).

Ramsey is a principal case within Fourth Amendment border search jurisprudence, as the Court addressed whether customs officials violated the Constitution by opening international letter mail based only on "reasonable cause" that the letter contained illegal contraband.[78] The majority rejected a distinction between international mail and other personal property such as luggage, based on the "longstanding recognition that searches at our border without probable cause and without a warrant are nonetheless reasonable."[79]

Although border searches are generally considered "reasonable" given the context, the Court has also noted, like Fourth Amendment jurisprudence as a whole, the "permissibility of a particular law enforcement practice is judged" by balancing the intrusion imposed on an individual's privacy interests against the practice's promotion of "legitimate governmental interests."[80] Yet, as previously noted, this ad-hoc balancing test in the border context is heavily weighted in the Government's favor.[81] Generally, routine searches at the border have consistently been upheld without any constitutionally-required finding of suspicion.[82]

However, a wrinkle in this Fourth Amendment balancing at the border emerged with the concepts of "routine" and "nonroutine" border searches.[83] The Court in *Montoya de Hernandez* addressed the actions of customs officials who detained a traveler suspected of smuggling narcotics in her alimentary canal.[84] Justice Rehnquist, writing for the

78. United States v. Ramsey, 431 U.S. 606, 611-16 (1977). Congress had granted Customs this power via statute, and thus the Court had only to determine whether the statute violated the Constitution, not whether "reasonable cause" was constitutionally required for the search. *Id.* at 615-16. The Court of Appeals had held that the border search exception was inapplicable to the routine opening of international mail, at this presented "too great a risk to personal privacy" without a showing of probable cause and securing a warrant. United States v. Ramsey, 538 F.2d 415, 421 (D.C.C. 1976), *rev'd,* 431 U.S. 606, (1977).

79. *Ramsey*, 431 U.S. at 619, 622 (internal quotations omitted). Searches at the border, the Court went on to discuss, are not based on exigent circumstances, but rather stand as their own categorical exception to the Fourth Amendment's warrant and probable cause requirements. *Id.* at 621-22. Therefore, border searches are reasonably simply because a person or item enters into the country. *Id.* at 619.

80. United States v. Villamonte-Marquez, 462 U.S. 579, 588 (1983) (internal citations omitted).

81. The Government's interest "is at its zenith at the international border." United States v. Flores-Montano, 541 U.S. 149, 152 (2004); *see also* United States v. Montoya de Hernandez, 473 U.S. 531, 540 (1985) ("…the Fourth Amendment balance between the interests of the Government and the privacy of the individual is … struck more favorably to the Government at the border.").

82. *See, e.g., Flores-Montano*, 541 U.S. at 155-56 (holding that "Government's authority to conduct suspicionless inspections at the border includes the authority to remove, disassemble, and reassemble a vehicle's fuel tank."); *see* United States v. Beras, 183 F.3d 22, 25-26 (1st Cir. 1999) ("routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant.") (internal citations omitted); *see* United States v. Molina-Isidoro, 884 F.3d 287, 291 (5th Cir. 2018 ("routine border searches may be conducted without any suspicion.").

83. *See Montoya de Hernandez*, 473 U.S. at 540.

84. *Id.* at 533-34.

majority, noted that the Court had yet to decide what level of suspicion would justify seizing a traveler "for purposes other than a routine border search."[85] The Court then held that, given the context, detention of a traveler at the border "beyond the scope of a routine customs search and inspection" is justified if it is based on reasonable suspicion.[86] Yet, in *Flores-Montano*, the Court criticized the lower court[87] for relying on the term "routine" to "fashion[] a new balancing test, and extend it to searches of vehicles."[88] Justice Rehnquist distinguished the use of "[c]omplex balancing tests" to determine what constitutes a routine search of vehicles as opposed "to a more 'intrusive' search of a person[.]"[89] Simply put, the "dignity and privacy interests" involved with the search of a person are not implicated in searches of vehicles.[90]

III. SEARCH OF ELECTRONIC DEVICES AT THE BORDER

As with Fourth Amendment jurisprudence more generally, the advent of technological advances has required courts to determine how the border exception squares with searches of electronic devices at the border.[91] Part A of this Section examines how federal courts have addressed the issue, discussing the development of federal court decisions that culminated in the recent split between the Fourth and Eleventh Circuits over whether reasonable suspicion is required to search digital devices. Although the bulk of this section focuses on how the judiciary has addressed this issue, Part B briefly examines the reactions of Congress and the Executive Branch.

---

85. *Id.* at 540 (citing United States v. Ramsey, 431 U.S. 606, 618, n.13 (1977) ("We do not decide whether, and under what circumstances, a border search might be deemed 'unreasonable' because of the particularly offensive manner in which it is carried out."). Subsequently, in *Flores-Montano* the Court left open the possibility that some property searches may be "so destructive" such that they might require a level of suspicion required for "highly intrusive" searches of people. 541 U.S. at 152, 155-56.

86. *Montoya de Hernandez*, 473 U.S. at 541. In a footnote, the majority was careful to note that they "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." *Id.* at 541, n. 4. As LaFave notes, the constitutional standard subsequently developed by federal courts regulating strip searches at the border requires "real suspicion," a standard lying between "mere suspicion" and probable cause. 5 LAFAVE, SEARCHES & SEIZURES AT §10.5(C). Practically speaking, the standard is essentially one requiring reasonable suspicion.

87. A panel of the Ninth Circuit summarily affirmed that removal of a vehicle's gas tank at the border required reasonable suspicion. United States v. Flores-Montano, No. 02-50306, 2003 WL 22410705, at *1 (9th Cir. Mar. 14, 2003) (relying on United States v. Molina-Tarazon, 279 F.3d 709 (9th Cir. 2002)), *rev'd,* 541 U.S. 149 (2004).

88. *Flores-Montano*, 541 U.S. at 152.

89. *Id.*

90. *Id.*

91. *See* United States v. Kolsuz, 890 F.3d 133 (2018); United States v. Touset, 890 F.3d 1227 (2018); *see also* Marion, *supra* note 6.

A. The Struggle to Define "Nonroutine" Border Searches in the Context of Electronic Devices

Searches of electronic devices at the border have increasingly drawn attention from legal scholars.[92] The Supreme Court has yet to address this specific issue, but almost every Federal Circuit that has concluded that suspicionless searches of electronic devices, such as laptops, cell phones, and cameras, do not violate the Fourth Amendment.[93] In light of the routine versus nonroutine search distinction, and *Flores-Montano*, most pre-*Riley* courts faced with these issues distinguished between searches of a person and those of inanimate objects.[94] In *United States v. Arnold*, the Ninth Circuit rejected the requirement of reasonable suspicion to search a traveler's laptop.[95] As the laptop was a piece of property, similar to the vehicle in *Flores-Montano*, the search did not "implicate the same dignity and privacy concerns as highly intrusive searches of the person."[96]

Determining whether a particular search of an electronic device was routine or nonroutine also contains another embedded issue, whether explicitly or implicitly contained in a court's determination: customs officials' method of obtaining the data.[97] Information stored on electronic devices can be accessed manually, similar to how a typical user would

92. *See, e.g.,* Miller, *supra* note 6 at 1943; Kugler, *supra* note 6 at 1165; Tom Rechtin, *Back to the Future of Your Laptop: How Backlash over Prolonged Detention of Digital Devices in Border Searches is Sympathetic of a Need for "Reasonable Suspicion" in All Border Searches of Digital Devices*, 7 THE CRIT: CRITICAL STUD. J. 66 (2014); Samuel A. Townsend, note, *Laptop Searches at the Border and United States v. Cotterman*, 94 B.U. L. REV. 1745 (2014); Sid Nadkarni, comment, *"Let's Have a Look, Shall We?" A Model for Evaluating Suspicionless Border Searches of Portable Electronic Devices*, 61 UCLA L. REV. 146 (2013); 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 (2017); Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403 (2013).

93. *See, e.g., Touset*, 890 F.3d at 1233; United States v. Linarez-Delgado, 259 Fed. Appx. 506, 508 (3rd Cir. 2007) (search of camcorder did not require a warrant, consent, or reasonable suspicion); *Ickes,* 393 F.3d 501, 505-06 (search of computer and computer disks did not require a warrant or probable cause); United States v. Arnold, 533 F.3d 1003, 1009-10 (9th Cir. 2008); *but see* United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013) (en banc); United States v. Kolsuz*,* 890 F.3d 133 (4th Cir. 2018).

94. *See* United States v. Arnold, 533 F.3d 1003, 1007-08 (9th Cir. 2008); *but see* United States v. Molina-Tarazon, 279 F.3d 709, 713 (9th Cir. 2002), *abrogated by* United States v. Flores-Montano, 541 U.S. 149 (2004) ("We hold . . . that some searches of inanimate objects can be so intrusive as to be considered nonroutine."); *see also* 5 LAFAVE, SEARCHES & SEIZURES at §10.5(F).

95. *Arnold*, 533 F.3d at 1008. The lower court utilized a sliding scale of intrusiveness to reach this conclusion. United States v. Arnold, 454 F. Supp.2d 999, 1002 (C.D. Cal. 2006), *rev'd*, 523 F.3d 941 (9th Cir. 2008*), amended and superseded on denial of reh'g*, 533 F.3d 1003 (9th Cir. 2008).

96. *Arnold*, 533 F.3d at 1008 (internal quotation marks omitted) (citing *Flores-Montano*, 541 U.S. at 152).

97. This line of reasoning stems from *Flores-Montano*, which some courts viewed as leaving open the possibility of a reasonable suspicion requirement for some searches of property. *See, e.g., Arnold*, 533 F.3d at 1009 (". . . there is nothing in the record to indicate that the manner in which the CBP officers conducted the search was 'particularly offensive[.]"). Thus, some courts began to focus on whether a specific search was "particularly offensive."

access the device.[98] Information can also be accessed through a forensic examination, which, as one scholar noted, typically involves the use of software programs to sort through the data contained on the device.[99]

Notably, five years after *Arnold,* the Ninth Circuit in *United States v. Cotterman*—which the court described as a "watershed case"—distinguished between cursory, manual searches and forensic searches by holding that a forensic examination of the defendant's computer at the border required reasonable suspicion.[100] Although recognizing a traveler's reduced expectation of privacy at the border and prevalent security concerns,[101] the court differentiated electronic devices from traditional types of property given the "private information" stored on these devices.[102] Yet more importantly, the forensic examination was the key factor, as the "comprehensive and intrusive nature" of the search warranted a requirement of reasonable suspicion."[103]

Post-*Riley*, two recent Federal Appellate decisions present two opposing views regarding forensic searches of electronic devices at the border.[104] Unlike pre-*Riley* cases, which focused more on the type of

98. *See Kolsuz*, 890 F.3d at 140. For example, a customs official would manually unlock an iPhone and access different applications on the cell phone, or search through a laptop by opening different files and folders contained on the laptop.

99. Forensic searches are performed by trained analysts and reveal "a wealth of information," including the data stored on the device and how the device has been used. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 537-38, 542 (2005). Perhaps more significantly, a forensic search allows analysts to unlock password-protected files, retrieve images viewed on the Internet, and restore deleted materials. United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013) (en banc). Recently, the Eleventh Circuit decided for the first time whether a warrant is required to forensically search a cell phone at the border. United States v. Vergara, 884 F.3d 1309 (11th Cir. 2018), *cert. denied*, No. 17-8639, 2018 WL 1993728 (U.S. Oct. 1, 2018). In a notably short opinion, the court held that a forensic search of a cell phone at the border requires neither probable cause nor a warrant. *Id.* at 1312. As petitioner only challenged whether probable cause was required, the court did not address whether reasonable suspicion was required. *Id.* at 1313.

100. *Cotterman*, 709 F.3d at 956, 968 ("An exhaustive forensic search of a copied laptop hard drive intrudes upon privacy and dignity interests to a far greater degree than a cursory search at the border."). The Defendant re-entered the United States from Mexico, where border agents were alerted of Defendant's prior conviction for use of a minor in sexual conduct, among other similar charges. *Id.* at 958. The Defendant's laptop was seized at the border, where border agents conducted an initial search as well as a follow-up forensic examination. *Id.* at 958-59. A divided panel of the court previously held that no reasonable suspicion was required for the forensic examination, which this en banc panel reversed. *See also* United States v. Saboonchi, 990 F. Supp. 2d 536, 569 (S.D. Cal. 2016) (holding that "a search of imaged hard drives of . . . [a smartphone and flash drive] taken from the Defendant at the border and subjected to forensic examination days or weeks later cannot be performed in the absence of reasonable suspicion.")

101. *Cotterman*, 709 F.3d at 963, 966.

102. *Id.* at 964. Comparing the case to *Montoya de Hernandez*, the court believed that "[t]he private information individuals store on digital devices—their personal 'papers' in the words of the Constitution—stands in stark contrast to the generic and impersonal contents of a gas tank . . .[l]aptop computers, iPads and the like are simultaneously offices and personal diaries."

103. *Id.* at 962, 964, 968.

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

search conducted, these two decisions focused on the nature of electronic devices more generally. In May 2018, the Fourth Circuit in *Kolsuz* confronted the constitutionality of a month-long, off-site forensic analysis of the defendant's iPhone after federal customs agents discovered firearms parts in defendant's luggage.[105] The majority's analysis began by recognizing the Supreme Court's "general guidance" regarding the distinction between "routine" and "non-routine," "highly intrusive" searches at the border.[106]

Upon review of applicable Circuit decisions, the majority concluded that the distinction between routine and nonroutine searches turns "primarily on how deeply it intrudes into a person's privacy."[107] Applying this principle to the forensic search of a cell phone, the court relied on *Riley*'s proposition that cell phones are "fundamentally different 'in both a quantitative and qualitative sense'" to distinguish cell phones from other objects traditionally subject to government searches.[108] "The sheer quantity of . . . uniquely sensitive" information on cell phones and other electronic devices, coupled with the ubiquitous nature of these devices, the court reasoned, makes it neither realistic nor reasonable for travelers to leave these digital devices at home when travelling.[109] As forensic searches allow governmental agents to analyze cumulatively the intimate details stored on electronic devices, the court held that these searches of

1227 (11th Cir. 2018).

105. *Kolsuz*, 890 F.3d at 136. The court only addressed the narrow issue of whether the forensic search of Defendant's phone was justified under the border search exception to the Fourth Amendment. *Id.* at 141. The forensic search, although limited to data stored on the phone itself, produced approximately 900 pages cataloguing Defendant's phone data. *Id.* at 136. Previously in 2012, governmental agents discovered 163 firearm parts in the Defendant's luggage as he attempted to board a flight to Turkey. *Id.* at 138. In this instance, agents discovered 18 handgun barrels, 22 9mm handgun magazines, four .45 caliber handgun magazines, and one .22 caliber conversion kit in the Defendant's two checked bags. *Id.* at 139.

106. *Kolsuz*, 890 F.3d at 144 (citing United States v. Flores-Montano, 541 U.S. 149, 152 (2004)). The court was careful to note that the Supreme Court had not "delineated precisely what makes a search nonroutine." *Id.*

107. *Id.* (citing United States v. Kolsuz, 185 F. Supp. 3d 843, 853 (E.D. Va. 2016). *See also* United States v. Uricoechea-Casallas, 946 F.2d 162, 166 (1st Cir. 1991) (applying reasonable suspicion standard to a strip search at the border); United States v. Sanders, 663 F.2d 1, 3 (2d Cir. 1981) (holding that a removal of artificial limb was nonroutine border search); Rivas v. United States, 368 F.2d 703, 709-10 (9th Cir. 1966) (holding that alimentary canal search was a nonroutine border search); United States v. Vega-Barvo, 729 F.2d 1341, 1349 (11th Cir. 1984) (holding that an x-ray was a nonroutine border search).

108. *Kolsuz*, 890 F.3d at 145-46 (quoting Riley v. California, 573 U.S. 373, 393 (2014)). The court was careful to note that "[t]he key to *Riley*'s reasoning is its express refusal to treat such phones as just another form of container." *Id.* at 145 (citing *Riley*, 573 U.S. at 391-96). *See also* United States v. Kim, 103 F. Supp. 3d 32, 51 (D.D.C. 2015) (highlighting the differences between digital devices and traditional types of containers); Alasaad v. Nielsen, No. 17-CV-11730-DJC, 2018 WL 2170323, at *16 (D. Mass. May 9, 2018) ("As an initial matter, the Court is not persuaded that *Riley*'s reasoning is irrelevant here simply because *Riley*'s holding was limited to the search incident to arrest exception[.]").

109. *Kolsuz*, 890 F.3d at 145 (citing United States v. Saboonchi, 990 F. Supp. 2d 536, 556 (D. Md. 2014)).

cell phones "must be treated as nonroutine border searches" and require some type of individualized suspicion, although the court declined to explicitly decide "whether reasonable suspicion is enough . . . or whether there must be a warrant based on probable cause[.]"[110] Warding off any potential concern of unworkability in this standard, the majority noted that CBP recently adopted a policy requiring reasonable suspicion for forensic searches of digital devices at the border.[111] However, in a concurring opinion, one judge criticized the majority's requirement of individualized suspicion, citing potential separation of powers concerns and arguing that the issue is better left to Congress and the Executive branch.[112]

In May 2018, the Eleventh Circuit again addressed a similar issue in *Touset*.[113] Border agents stopped the defendant after he arrived on an international flight and detained the defendant's electronic devices, later conducting forensic searches and finding child pornography.[114] In contrast to *Kolsuz*, the court spent considerable time discussing the history of the border search exception, reiterating that the Supreme Court has never required reasonable suspicion for a search of property at the border.[115] Thus, the court refused to analogize searches of electronic

110. *Id.* at 145-46 (citing United States v. Jones, 565 U.S. 400, 415 (2011) (Sotomayor, J., concurring)). In this instance, however, the court went on to uphold the search because under the circumstances "it was reasonable for the CBP officers who conducted the forensic analysis of Kolsuz's phone to rely on the established and uniform body of precedent allowing warrantless border searches of digital devices that are based on at least reasonable suspicion." *Id.* at 148. Given *Kolsuz*'s outcome and unique holding that only *some form* of individualized suspicion is required, while declining to determine precisely what the correct level of suspicion should be (i.e. reasonable suspicion or probable cause), has led some courts to interpret *Kolsuz* differently. *See* United States v. Touset, 890 F.3d 1227, 1234 (11th Cir. 2018) (interpreting *Kolsuz* as requiring at least reasonable suspicion for forensic searches of electronic devices at the border); *but see* United States v. Cano, 934 F.3d 1002, 1016 (9th Cir. 2019) (stating *Kolsuz* "declin[ed] to decide whether the [measure of individualized suspicion] should be reasonable suspicion or probable cause.").

111. *Kolsuz*, 890 F.3d at 146; *see* CBP Directive No. 3340-049A, *supra* note 9.

112. The majority, the concurring opinion argued, appears to have left the "legislative and executive branches shivering in the cold." *Kolsuz*, 890 F.3d at 148 (Wilkinson, J., concurring in the judgment). Due to the executive's "strong sovereign interest" at the border, the majority should simply have assumed reasonable suspicion, even if required, was present, and simply stopped any further inquiry. From this perspective, searches at the border "should be principally a legislative question," calling for the "greatest caution and circumspection" by courts. *Id*.

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

114. *Id.* at 1230. As in *Kolsuz*, agents first manually searched the Defendant's two iPhones and camera, detaining only Defendant's two laptops, two external hard drives, and two tablets. *Id.* Child pornography was found on one of the laptop computers, Unites States v. Touset, No. 1:15-CR-45-MHC, 2016 WL 11432531, at *2 (N.D. Ga. Jan. 6, 2016), and the Government charged under 18 U.S.C. §2252(a) and (b) for knowingly receiving child pornography, knowingly transporting and shipping child pornography, and knowingly possessing a computer and computer-storage device containing child pornography. *Touset*, 890 F.3d at 1231.

115. *Touset*, 890 F.3d at 1232-33 ("We see 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."); *See also* United States v. Flores-Montano, 541 U.S. 149, 152 (2004) ("the reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches

devices to a "highly intrusive search[] of a person's body."[116] Reasoning from *Boyd v. United States*,[117] the court noted that the search of a traveler's property at the border is a long-standing practice deeply associated with excluding illegal articles from the country.[118] The court found it illogical to place "special treatment" on electronic devices because of their prevalence or storage capacities due to border agents' "same responsibility for preventing importation of contraband in a traveler's possession regardless of advances in technology."[119] Searches of electronic devices simply do not, the court reasoned, implicate the same intrusions of privacy and violations of personal indignity as does a search of a person's body.[120]

Similarly, the majority was not persuaded with conflicting holdings reached by the Fourth and Ninth Circuits, as *Riley*'s narrow holding is inapplicable to border searches.[121] Citing *Kolsuz'*s concurring opinion, the court called for judicial restraint given the "dangers of judicial standard-setting in an area as sensitive as border searches[.]"[122] The majority went on to distinguish *Riley*'s reasoning; in searches incident to arrest, digital devices do not implicate the concerns underlying the exception—harm to officers or destruction of evidence.[123] Yet the concern of unlawful entry of illegal contraband that underlies *Riley*'s reasoning is still implicated by digital data[124] The court recognized that,

---

of the person – dignity and privacy interests of the person being searched – simply do not carry over to vehicles."); United States v. Thirty-Seven Photographs, 402 U.S. 363, 376 (1971) (traveler's "right to be let alone neither prevents the search of his luggage nor the seizure of unprotected, but illegal, materials when his possession of them is discovered during . . . a search.").

116. *Touset*, 890 F.3d at 1234 (citing United States v. Alfaro-Moncado, 607 F.3d 720, 729 (11th Cir. 2010)).

117. 116 U.S. 616.

118. *Touset*, 890 F.3d at 1233 (citing Boyd v. United States, 116 U.S. 616 (1886); *Thirty-Seven Photographs*, 402 U.S. 363). It is also noteworthy that the *Riley* Court mentioned the "absen[ce] . . . [of] precise guidance from the founding era." Riley v. California, 573 U.S. 373, 385 (2014). Arguably, cases such as *Boyd* established this type of precise guidance.

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

120. *Id.* at 1234. The Eleventh Circuit had previously identified three factors to distinguish highly intrusive searches: (1) physical contact between the searcher and the person searched, (2) exposure of intimate body parts, and (3) use of force. United States v. Vega-Barvo, 729 F.2d 1341, 1346 (11th Cir. 1984).

121. *Touset*, 890 F.3d at 1234 (citing United States v. Vergara, 884 F.3d 1309, 1312-13 (11th Cir. 2018) (concluding that *Riley*'s holding is expressly limited to search-incident-to-arrest exceptions and that border searches have historically been excluded from warrant and probable cause requirements).

122. *Id.* at 1237 (citing United States v. Kolsuz, 890 F.3d 133, 150 (4th Cir. 2018) (Wilkinson, J., concurring in the judgment)). Instead of "charging unnecessarily ahead," the majority felt that the "adaptable legislative process" would provide "practical insights and experience to the inquiry," particularly given the historical practice of "deferring to the legislative and executive branches." *Id.* (citing *Kolsuz*, 890 F.3d at 153 (Wilkinson, J., concurring in the judgment).

123. *Touset*, 890 F.3d at 1235 (citing *Riley*, 573 U.S. at 384-87).

124. *Id.* at 1235.

if anything, technological advances such as electronic devices provide ample means for concealing contraband, and thus requiring reasonable suspicion for these searches would "create special protection for the property most used to store and disseminate child pornography."[125]

B. Administrative and Congressional Reactions

As noted in both *Kolsuz* and *Touset,* digital device searches at the border implicate both the Legislative and Executive branch, and this issue has not gone unnoticed by either branch. In August 2009, CBP issued a policy directive to provide guidance and standard operating procedures regarding border searches of electronic devices.[126] The 2009 Directive stated that in the context of a border search, examination of electronic devices and review or analysis of digitally stored information requires no level of suspicion, reflecting the general consensus among federal courts at that time.[127] However, in January 2018, CBP issued a superseding Directive governing electronic searches at the border.[128] In contrast to the 2009 Directive, the 2018 Directive differentiated between a "basic search," which requires no suspicion, and an "advanced search," which requires reasonable suspicion, with the latter referring to the use of external equipment to "review, copy, and/or analyze" digital contents.[129]

Concerns regarding these searches at the border have also found voice within the Legislative branch. In April 2017, Senator Ron Wyden introduced a bill that would prohibit all digital border searches conducted without a warrant.[130] And in February 2018, Senator Patrick Leahy introduced a bill that would require reasonable suspicion for manual searches and a warrant supported by probable cause for forensic searches.[131] Both bills were referred to the Senate Committee on

125. *Touset*, 890 F.3d at1235. The Eastern District of New York had previously expressed similar sentiments. *See* Pascal Abidor, National Association of Criminal Defense Lawyers v. Johnson, No. 10-CV-4059 (ERK), 2016 WL 3102017, at *6 (E.D.N.Y. June 2, 2016) ("Applying the holding in *Riley* in this context would significantly, if not totally, undermine [the purposes of a border search.]").

126. U.S. CUSTOMS AND BORDER PROT., DIRECTIVE NO. 3340-049, https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf.

127. *Id.* at 3.

128. U.S. CUSTOMS AND BORDER PROTECTION, DIRECTIVE NO. 3340-049A, *supra* note 9.

129. *Id.* at 4-5. Although the Directive suggests greater protections for the privacy of international travelers, some attorneys have criticized the Directive for lack of guidance and argued "[t]here's not a lot of confidence" that the policy is actually being followed. Brandi Buchman, *Committee Examines Border Patrol's Phone Searches*, COURTHOUSE NEWS SERVICE (July 11, 2018) (quoting Neema Singh Guliani), https://www.courthousenews.com/committee-examines-border-patrols-phone-searches/.

130. S. 823, 115th Cong. (2018). The Protecting Data at the Border Act would allow an exception for such searches in the case of an "emergency situation." The bill would also prohibit denial of entry into the United States if a traveler refuses to give consent for a digital search.

131. S. 2462, 115th Cong. (2018).

Homeland Security and Governmental Affairs.[132] In July 2018 the Senate Subcommittee on Federal Spending Oversight and Emergency Management held a hearing regarding warrantless smartphone searches at the border.[133] As of now, no further action has been taken on either proposed bill.

Needless to say, digital device searches at the border have become a difficult issue for the courts, particularly in the post-*Riley* world. Yet as the following section suggests, analysis of *Kolsuz* and *Touset* demonstrates that reasonable suspicion is constitutionally required for digital device searches at the border.

IV. DISCUSSION

The split between the Fourth and Eleventh Circuits regarding what level of suspicion, if any, is required for forensic searches of electronic devices at the border might at first glance appear to be a straightforward, niche constitutional issue. However, given the intersection of two subsets of Fourth Amendment jurisprudence—the longstanding border search exception and how courts grapple with technological advances—both Circuits' approaches raise questions about the zeitgeist of law, technology, and privacy.[134] And, more specifically, both approaches raise the question of how technological advances impact the sensitive area of sovereign concerns at the border, if they do at all. The crux of the issue concerns both how to interpret *Riley* and how to distinguish between routine and nonroutine searches.

The following section suggests that *Kolsuz* arrived at the correct conclusion—the Fourth Amendment requires some measure of individualized suspicion for forensic searches of electronic devices at the border—but should have gone further by explicitly adopting the reasonable suspicion standard. *Riley* plays a fundamental role in this debate and, as such, part A of this subsection analyzes the differing interpretations of *Riley* and the associated implications with each approach. Part B dissects the split between *Kolsuz* and *Touset,* and suggests why *Kolsuz* presents the constitutionally-appropriate approach and correctly interprets *Riley*. Part C then explains why even in light of *Riley* and *Kolsuz*, only reasonable suspicion should be required for

132. *See* S. 823, 115th Cong., https://www.congress.gov/bill/115th-congress/senate-bill/823; *see also* S. 2462, 115th Cong., https://www.congress.gov/bill/115th-congress/senate-bill/2462/all-info.

133. *Examining Warrantless Smartphone Searches at the Border: Hearing on S. 2462 Before the S. Subcomm. on Fed. Spending Oversight and Emergency Mgmt.,* 115th Cong. 1.

134. Kerr notes that when technology threatens privacy, the prevailing zeitgeist has been for the courts and the Constitution to take an active role and offer the primary response. However, Kerr goes on to argue that more judicial caution is required in favor of a more legislative regulation of government's technology use. Kerr, *supra* note 48 at 803, 804-05.

forensic searches. Finally, Part D explores potential challenges lower courts might continue to face moving forward, and suggests expanding a reasonable suspicion requirement for manual searches of electronic devices as well.

A. Potential Impacts of Riley on Border Searches of Electronic Devices

As the Supreme Court has yet to address search of electronic devices at the border, a crucial question for lower courts in the post-*Riley* world is what effect, if any, *Riley* has on the border search exception. Analyzing *Riley*, there are three potential interpretations that implicate search of electronic devices at the international border: (1) a strict interpretation, (2) a methodological interpretation, and (3) a categorical interpretation creating a doctrinal change.

1. A Strict Interpretation of *Riley*

From a strict interpretation viewpoint, *Riley* is limited only to the search incident to arrest exception.[135] The majority only concerned itself with how the search incident to arrest exception applies to modern cell phones and nothing else.[136] And as Chief Justice Roberts was careful to note, the holding was not expansive; rather, the holding was limited to generally requiring a warrant before a cell phone is searched incident to arrest.[137] Further clarifying this holding, the majority also noted that other case-specific exceptions or exigencies could also justify warrantless searches of a cell phone.[138]

Through closer analysis, even *Riley*'s line of reasoning suggests a limitation to this particular exception to the warrant requirement,[139] as the underlying justifications for searches incident to arrest were not present with cell phones. First, searches of cell phone data categorically do not implicate concerns of officer safety. Unlike unknown objects in a physical container, digital data cannot immediately harm officers present during

135. *See* United States v. Saboonchi, 48 F. Supp.3d 815, 818 (D. Md. 2014) (denying Defendant's motion to reconsider based on the Supreme Court's recent decision in Riley v. California, 573 U.S. 373 (2014)) ("Beyond exigencies, *Riley* makes no specific reference to the border search exception or any other case-specific exceptions to the warrant requirement previously announced by the Court other than to clarify that they remained intact.") Noting the narrowness of *Riley*'s holding, the Fifth Circuit affirmed the admission of evidence seized from a defendant's cellphone without a warrant based on the good-faith exception. *See* United States v. Molina-Isidoro, 884 F.3d 287, 292-93 (5th Cir. 2018).

136. Riley v. California, 573 U.S. 373, 384-86 (2014).

137. *Id*. at 401.

138. *Id.* at 401-03.

139. *See* Miller, *supra* note 6 at 1987.

the arrest.[140] Second, there is no concern of preventing the destruction of evidence. As both parties conceded, officers could have seized the cell phone incident to arrest to prevent the destruction of any incriminating digital evidence.[141] Non-electronic evidence within the arrestee's grasp, on the other hand, always presents the possibility of being destroyed before a later seizure. Thus, a strict reading of *Riley*, both from its holding and reasoning, demonstrates a formal limitation only to the search incident to arrest exception.

2. A Methodological Interpretation of *Riley*

Riley can also be read as presenting a slight methodological shift in Fourth Amendment analysis in light of the digital age, particularly in regards to individuals' cell phones and other electronic devices.[142] Although the majority was concerned with the search incident to arrest exception, the core of the opinion builds from how to reconcile electronic devices with the then-controlling law of searches incident to arrest. After all, a "mechanical application" of precedent could have easily supported the warrantless search.[143] Intertwined with the discussion of how electronic devices do not implicate the underlying rationale of the search incident to arrest exception is a broader recognition that in the digital age, a formal and mechanical application of precedent is often inadequate to properly interpret the reasonableness of a given search.[144] This interpretation suggests a generally more cautious approach when evaluating the reasonableness of a search of an electronic device.

3. A Categorical Interpretation of *Riley*

Within the methodological interpretation lies yet another more forceful approach: viewing cell phones as categorically different from traditional, tangible objects historically subject to government searches. From this line of reasoning, *Riley* stands for the proposition that for Fourth Amendment purposes, cell phones and electronic devices should be treated as distinct from traditional physical containers. This interpretation stems from the majority's recognition that categorically, cell phones implicate heightened privacy concerns due to the exposure of digital

140. *Riley*, 573 U.S. at 387-89.

141. *Id*. at 387-89.

142. *See* Miller, *supra* note 6 at 1996.

143. *Riley*, 573 U.S. at 385-86.

144. *See Id.* at 384-87. As Justice Alito was concerned, "we should not mechanically apply the rule used in the pre-digital era to the search of a cell phone." *Id.* at 406-07 (Alito, J., concurring in part and concurring in the judgment).

data.[145] Even from the outset, treating a cell phone as a container "is a bit strained as an initial matter."[146] Chief Justice Roberts recognized that cell phones "differ in both a quantitative and a qualitative sense" from other tangible objects.[147]

Quantitatively, the immense storage capacity of cell phones greatly broadens the scope of an intrusion on privacy.[148] In addition to the mere technological capabilities, cell phones also allow the accumulation of varying types of information.[149] In this sense, the intrusion on privacy is no longer physically limited as searches of non-electronic containers and objects are. A search of a bag or purse simply does not reveal the amount of information as would a search of a cellphone. Qualitatively, the nature of data stored on cell phones is distinctly different from physical records. Although electronic devices can reveal evidence of illegal activities,[150] the aggregate information obtained from apps, photographs, internet search history, text messages, and call logs, when taken together, can form a "revealing montage of the user's life."[151] Following this logic, both cell phones and other similar electronic devices such as tablets and laptops tilt the Fourth Amendment reasonableness balance towards a heightened privacy interest of citizens.

B. Why Kolsuz Got It Right: The Shortcomings of a Traditional Approach to Forensic Examinations of Electronic Devices at the Border

In the post-*Riley* world, and the digital age more generally, courts have struggled to determine the proper constitutional protections for electronic devices at the border. *Kolsuz* and *Touset* offer a perspective on two differing approaches to the issue. At a baseline, these cases can both be understood as a conflict over the correct approach of determining what

145. *Id.* at 393-94 (majority opinion).

146. Not to mention the ability to use cloud computing to access remotely stored digital information not actually stored on the cell phone. *Id.* at 397-98.

147. *Id.* at 393.

148. The Court correctly noted that the "gulf between physical practicality and digital capacity" would continue to widen. *Id.* at 394. At the time *Riley* was decided, the standard capacity of the highest selling smart phone was 16 gigabytes. *Id.* Now, the standard capacity of an iPhone 8 is 64 gigabytes, with a maximum capacity of 256 gigabytes. Apple Store, https://www.apple.com/iphone-8/specs/. The upcoming iPhone Xs has a maximum capacity of 512 gigabytes. Apple Store, https://www.apple.com/iphone-xs/specs/.

149. "Much of the information stored in a person's cellular phone is deeply personal. The information can include photographs, text messages, e-mails, personal notes, records of visited websites, and many other kinds of personal information." Kerr, *supra* note 92 at 405.

150. For example, a search of a cell phone can reveal child pornography, classified government information, communications evidencing narcotics distribution, or videos or pictures implicating an individual in a homicide.

151. *Riley*, 573 U.S. at 395-96 (internal citations omitted).

constitutes a "routine" or "nonroutine" border search, a distinction that emerged in *Montoya de Hernandez* but was subsequently narrowed by the Supreme Court in *Flores-Montano*. *Touset* represents a more traditional application of the border search exception, simply encompassing electronic devices into the more traditional forms of property traveling across borders and following a strict interpretation of *Riley*.[152] *Kolsuz* holds out electronic devices as fundamentally different from tangible objects traditionally subject to searches at the border, utilizing the second and third interpretation of *Riley*.[153] As the following analysis suggests, the Fourth Circuit's approach in *Kolsuz* is both the preferred and constitutionally-appropriate conclusion.

Importing *Riley*'s reasoning into the border search context is logically appropriate. Regarding an expectation of privacy, arrestees and international travelers are in similar situations as their respective situations leave them with reduced privacy interests.[154] Upon arrest, an arrestee is in custody of the state, and for national security purposes, international travelers are subject to certain security searches. Additionally, the *Riley* majority was particularly concerned with the pervasiveness of cell phones. Chief Justice Roberts described the ubiquitous nature of cell phones in an interesting manner, concluding that cell phones are such a "pervasive and insistent part of daily life that the proverbial visitor from Mars" might believe they are an important part of our anatomy.[155] This concern is even greater at the border, as it is both unrealistic and unreasonable to expect an average traveler to leave their digital device at home while traveling.[156] *Touset* proposes that travelers are free to simply leave these devices at home, as they are on notice that a search may be made at the border.[157] While this is true, and travelers do have a reduced expectation of privacy,[158] requiring a traveler to leave her electronic devices at home to protect her digital information from a potential forensic search by customs officials seems unrealistic. Particularly given the international component of the travel, travelers use their electronic devices for a number of necessary reasons, such as keeping in touch with loved ones, documenting their trip, and tending to

152. *See* United States v. Touset, 890 F.3d 1227, 1233-35 (11th Cir. 2018). Circuit precedent only required reasonable suspicion for "highly intrusive searches of a person's body" at the border. *Id.* at 1234 (citing United States v. Alfaro-Moncado, 607 F.3d 720, 729 (11th Cir. 2010)).

153. *See* United States v. Kolsuz, 890 F.3d 133, 144-46 (4th Cir. 2018).

154. *See Riley*, 573 U.S. at 391-92; United States v. Montoya de Hernandez, 473 U.S. 531, 539-40 (1985).

155. *Riley*, 573 U.S. at 385.

156. *See Kolsuz*, 890 F.3d at 145 (citing United States v. Saboonchi, 990 F. Supp. 2d 536, 556 (D. Md. 2014)).

157. *Touset*, 890 F.3d at 1235.

158. *Id.*

work obligations.

By failing to recognize any impact of *Riley*, the *Touset* majority's reasoning demonstrates the shortcomings of utilizing a traditional application of the border search exception when analyzing forensic searches of electronic devices. *Touset* presents a strong argument in favor of limiting *Riley*'s reasoning in the border-search context. This is because, at a certain level, *Riley*'s underlying rationale fails to support a requirement of reasonable suspicion at the border. Key to *Riley*'s outcome was that the reasonableness balancing test tilted in favor of individual privacy interests; cell phones were "untethered" from the weighty governmental interests of officer safety and preventing the destruction of evidence.[159] Requiring probable cause would therefore not infringe the government's legitimate interests. Thus, in the context of searches incident to arrest, the reasonableness of searching cell phones fell in favor of protecting individuals' heightened privacy interest. Yet as *Touset* correctly notes, the presence of electronic devices at the border does not reduce the governmental interests. In fact, the increasing use of electronic devices actually facilitates the transfer of contraband, particularly child pornography, across the border.[160] Requiring reasonable suspicion at the border would therefore hinder the government's weighty interest of preventing the flow of contraband, much unlike the balance in *Riley*.

Notwithstanding the governmental interest, *Touset*'s reasoning fails to recognize *Riley*'s other implications regarding cell phones and other electronic devices.[161] *Riley* can and should have a more nuanced application in the context of border searches, as demonstrated through *Kolsuz*. Considering only the strictly formal impact of *Riley* ignores the broader implications regarding the Fourth Amendment and technological advances, and effectively unhinges the Fourth Amendment from reality and society's ordinary expectations. The effect is demonstrated through the personal accounts of travelers being "humiliated and shaken" by these searches.[162] Moreover, although the Eleventh Circuit had previously been unwilling to "distinguish between different kinds of property,"[163] cell

159. *See Riley*, 573 U.S. at 385-86.

160. "Indeed, if we were to require reasonable suspicion for searches of electronic devices, we would create special protection for the property most often used to store and disseminate child pornography." *Touset*, 890 F.3d at 1235. *See* Brief of Appellee at 29, *Kolsuz*, 890 F.3d 133 (No. 16-4687) ("[T]he greater storage capacity of electronic devices enables greater harm through the smuggling of" contraband).

161. Although *Riley* only addressed cell phones, the analysis is just as applicable to laptops, tablets, and other similar electronic devices, as all of these items are still quantitatively and qualitatively different from non-electronic tangible items.

162. *See* Savage and Nixon, *Privacy Complaints Mount*, NEW YORK TIMES (Dec. 22, 2017), https://www.nytimes.com/2017/12/22/us/politics/us-border-privacy-phone-searches.html.

163. United States v. Touset, 890 F.3d 1227, 1233 (11th Cir. 2018). The majority cited *Flores-Montano*'s rejection of a judicial attempt to distinguish between routine and nonroutine searches of a

phones and electronic devices are not typical forms of property. *Riley* logically and realistically recognized how modern cell phones are categorically distinguishable from objects traditionally subject to government searches.[164] By mechanically applying precedent, *Touset* effectively disregards the true nature of electronic devices and demonstrates the shortcomings of utilizing a traditional application of the border search exception.[165] Continuing such a distinction will inevitably lead to a narrowing of rights and the "detriment of individual liberty."[166]

A large part of the issue arguably lies with how to determine what constitutes a nonroutine border search. *Kolsuz* posits that the determination is "focused primarily on how deeply . . . [the search] intrudes into a person's privacy."[167] In contrast, *Touset* focuses on "the indignity that will be suffered by the person being searched."[168] Yet as *Touset* also draws a firm line between searches of persons and property, personal indignity is largely framed in terms of physical indignity.[169] The Eleventh Circuit's mechanical application of precedent and bright-line between property and persons prevents the recognition that searches of tangible items, such as luggage, are fundamentally different from searches of electronic devices.[170] Although there is inevitably some form

vehicle, as well as a Ninth Circuit opinion upholding a suspicionless search of a crew member's living quarters on a foreign cargo ship. *Id.* (citing United States v. Flores-Montano, 541 U.S. 149, 152 (2004), United States v. Alfaro-Moncado, 607 F.3d 720, 727 (11th Cir. 2010)). However, the Third Circuit had required reasonable suspicion for a border search of a passenger cabin on a cruise ship. United States v. Whitted, 541 F.3d 480, 488 (3rd Cir. 2008). Interestingly, *Riley* might even offer a counter-argument diminishing the impact of this analogy: "In 1926, Learned Hand observed . . . that it is 'a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him.' If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is." Riley v. California, 573 U.S. 373, 396-97 (2014) (internal citations omitted) (emphasis in original).

164. *See Riley*, 573 U.S. at 391-94.

165. *Touset* relied on Circuit precedent, which drew a bright-line rule distinguishing property from persons. *Touset*, 890 F.3d at 1234 (citing *Alfaro-Moncado*, 607 F.3d at 732).

166. Donohue, *supra* note 46 at 678.

167. *Kolsuz*, 890 F.3d at 144 (internal citation omitted).

168. *Touset*, 890 F.3d at 1234 (citing *Vega-Barvo*, 729 F.2d at 1345).

169. The Eleventh Circuit considers three factors that contribute to the personal indignity endured by the person searched: (1) physical contact between the searcher and the person searched, (2) exposure of intimate body parts, and (3) use of force. *Touset*, 890 F.3d at 1234 (citing United States v. Vega-Barvo, 729 F.2d 1341 (11th Cir. 1984)).

170. *See Kolsuz,* 890 F.3d at 144-46; *see also* United States v. Kim, 103 F. Supp. 3d 32, 51 (D.D.C. 2015) ("I cannot help but find that even if a computer or cell phone is analogized to a closed container, a forensic search cannot be analogized to a conventional search of luggage or even of a person. A forensic search is far more invasive than any other property search that I have come across and, although it lacks the discomfort or embarrassment that accompanies a body-cavity search, it has the potential to be even more revealing.") (citing United States v. Saboonchi, 990 F. Supp. 2d 536, 568 (D. Md. 2014)).

of indignity suffered from either search, combing over the personal effects within a suitcase is drastically different from a government official perusing through one's electronic device.[171] While such an inquiry would have been appropriate before *Riley*, it is hard to believe that, post-*Riley*, the search of an electronic device does not implicate any personal indignity.[172] Cell phones and laptops represent a digital version of their owners—their "digital selves." These devices "possess[] a greater measure of personhood" than traditional, non-electronic property.[173] Unlike other physical "containers," electronic devices are more akin to an extension of the owner, which from a metaphysical sense can explain why a traveler having such a device searched experiences a feeling of privacy invasion.[174]

Kolsuz's focus on privacy concerns more generally recognizes that in the digital age, personal indignity can be implicated at the border outside of a search of a person. Cell phones and laptops allow individuals to carry a "cache of sensitive personal information,"[175] information that "contain[s] the most intimate details" of individuals' lives.[176] Although searching an electronic device might not rise to the level of indignity suffered by the search of one's person, a fairly high level of indignity is still suffered.[177] By searching cell phones or laptops, customs officials

171. A search of luggage and the physical items within can elicit feelings of embarrassment and violations of privacy, as one's undergarments or letters can be revealed. A search of a cell phone or laptop also reveals functional equivalents of physical items, such as photographs or emails. However, a traveler likely feels a higher degree of privacy in the information stored on electronic devices, which is demonstrated by passwords placed on these devices. Moreover, electronic devices can also reveal an individual's activities, such as browsing history.

172. One scholar conducted an empirical study measuring the perceived intrusiveness of electronic-device searches and the actual expectations of ordinary citizens. Summarizing the findings, the author concluded "[e]lectronic-device searches are seen as among the most intrusive of those described in the current case law. They are the most revealing of sensitive information. They are only less embarrassing than strip searches and body cavity searches." Kugler, *supra* note 6 at 1211.

173. Rechtin, *supra* note 92 at 87. Distinguishing electronic devices from the gas tank in *Flores-Montano* to electronic devices, Rechtin argues that cell phones and laptops have a "dual life." Digital devices not only serve as a container of "matter," but also have the "ability to embody and transmit the person's thoughts and expressions" and thus serve as "an extension and embodiment of the person who owns it." *Id.* at 87-88.

174. *See Id.; see also* Savage and Nixon, *supra* note 162.

175. Riley v. California, 573 U.S. 373, 395 (2014).

176. United States v. Kolsuz, 890 F.3d 133, 145 (4th Cir. 2018) (citing United States v. Cotterman, 709 F.3d 952, 964 (9th Cir. 2013) (en banc)). As one scholar noted, "[i]t's no exaggeration to say that unfettered access to a cellphone allows investigators to uncover details about almost every intimate communication and relationship associated with the owner of the cell phone." *Examining Warrantless Smartphone Searches at the Border: Hearing on S. 2462 Before the S. Subcomm. on Fed. Spending Oversight and Emergency Mgmt.,* 115th Cong. 1 (testimony of Matthew Feeney, Director, Project on Emerging Technologies at the Cato Institute).

177. It is also important to note that when electronic devices are searched, the traveler is either detained or free to leave without their device. *See* Alasaad v. Nielsen, No. 17-CV-11730-DJC, 2018 WL 2170323, at *5-8 (D. Mass. May 9, 2018). These measures only add to the indignity suffered when

have access to sensitive text messages and emails, private photographs, and Internet search history.[178]

The fact that *Kolsuz* and *Touset* addressed forensic searches simply exacerbates the issue of privacy. Such "comprehensive forensic analysis" of digital devices reveals an "unparalleled" amount of information.[179] And unlike a manual search, forensic searches generate reports that cumulatively analyze all of the data stored on an electronic device.[180] It is not difficult to imagine that a traveler who is forced to allow customs officials to forensically search their phone or laptop will experience a range of emotions such as anger, humiliation, or personal offense. Taking *Kolsuz* as an example, the forensic analysis generated an 896-page report including the Defendant's photos, videos, emails, messenger conversations, call log, and calendar.[181] By adhering to a strict property/person distinction, the decision in *Touset* allows customs officials to gain all of this information without any individualized suspicion that a traveler was involved in criminal activity.[182]

An argument can be made that requiring reasonable suspicion for forensic searches in effect allows greater protections for electronically stored photographs than for physical copies of photographs carried across the border, but such an argument misses the point. With hard copies of photos, travelers intentionally choose which images will accompany them on their travelers. Whereas with electronic images, travelers carrying their cell phone or laptop travel with hundreds or thousands of photos that are contained on these devices. There is no cognition, no decision-making involved in which photos are taken on a certain travel and which photos are left behind. The same holds true for other digitally stored data, such as emails and text messages.

Kolsuz's conclusion that some form of individualized suspicion is required for forensic searches of electronic devices demonstrates the proper analysis of the issue in light of *Riley*. Despite the long-standing border search exception, modern electronic devices implicate greater privacy concerns for the traveler, shifting the reasonableness balance in favor of the traveler and thus requiring reasonable suspicion to search the traveler's electronic devices. As *Riley* noted, when privacy-related

suspicionless digital device searches are conducted.

178. *Id.* at 145; *see also Riley*, 573 U.S. at 395-96. For example, two of the plaintiff's in *Alasaad* had their phone searched, which revealed photos of the plaintiffs without their headscarf. 2018 WL 2170323, at *5-7.

179. *Kolsuz*, 890 F.3d at 145.

180. *Id.*

181. *Id.* at 139.

182. *Touset*'s majority goes on to note that "[a]lthough it may intrude on the privacy of the owner, a forensic search of an electronic device is a search of property. And out precedents do not require suspicion for intrusive searches of any property at the border." 890 F.3d at 1234 (internal citation omitted).

concerns are weighty enough, this can overcome the diminished expectation of privacy an individual might have.[183] Given the inherently sensitive nature of data stored on electronic devices, combined with this information being forensically searched, the Fourth Amendment must protect travelers from such searches conducted without reasonable suspicion.

C. Reasonable Suspicion Should Be Required to Perform a Search of a Traveler's Electronic Devices

Although *Kolsuz* leaves open the possibility that a higher standard than reasonable suspicion could be required for forensic searches at the border, reasonable suspicion is the correct standard to apply.[184] For although *Riley*'s reasoning influences the border search exception, due weight must still be given to the exception's justifying principles and the longstanding recognition of the government's strong interests at the border.[185] Given *Riley*'s narrow holding, the opinion should not be understood as a categorical rule requiring probable cause or a warrant whenever government officials seek to search electronic devices.[186] *Riley* should instead be read as demonstrating a doctrinal shift: searches of electronic devices implicate heightened privacy concerns that need to be given due weight in the reasonableness balancing.[187]

Even though forensic searches of electronic devices are invasive actions infringing traveler's Fourth Amendment privacy interests, the government's interest at the border is still at its "zenith."[188] And as *Touset* correctly notes, the emergence of the digital era still implicates traditional and legitimate governmental concerns.[189] As an example, consider a traveler who possesses child pornography and is attempting to board an international flight. In the pre-digital age, CBP or ICE officials could

183. Riley v. California, 573 U.S. 373, 391-93 (2014) (internal citation omitted).

184. *But see* Miller, *supra* note 6 at 1996 (concluding that post-*Riley*, digital border searches should be treated as nonroutine and require reasonable suspicion *or* probable cause).

185. *See, e.g.,* Boyd v. United States, 116 U.S. 616, 623 (1886); United States v. 12 200-Ft. Reels of Super 8mm. Film, 413 U.S. 123, 125 (1973); United States v. Ramsey, 431 U.S. 606, 620 (1977).

186. *But see* United States v. Vergara, 884 F.3d 1309, 1313-19 (11th Cir. 2018) (Pryor, J., dissenting) (post-*Riley*, forensic search of phone at the international border requires a warrant based on probable cause).

187. This interpretation explains Chief Justice Roberts' discussion of why exigencies could allow warrantless searches of cell phones. Riley v. California, 573 U.S. 373, 401-03 (2014). Exigencies increase the government's interest under the specific circumstances, thus again re-shifting the reasonableness balancing.

188. United States v. Flores-Montano, 541 U.S. 149, 153 (2004) (internal citation omitted).

189. "[T]he government interest in stopping contraband at the border does not depend on whether child pornography takes the form of digital files or physical photographs." United States v. Touset, 890 F.3d at 1227, 1235 (11th Cir. 2018).

search the traveler's suitcase, without any level of suspicion, and uncover the child pornography. However, in the digital age, if electronic devices receive a higher degree of protection from searches and child pornography is stored on the traveler's cell phone, the child pornography will be subject to greater Fourth Amendment protections merely because it is stored digitally. Thus, *Riley* cannot be fully applicable, and probable cause or a warrant cannot/should not be constitutionally required, as there is no lessened governmental interest in these situations. Rather, as previously noted, due to the heightened privacy interest in electronic devices, the determination of reasonableness must be re-balanced. Determining that, as a constitutional matter, probable cause or a warrant is required would ignore the governmental side of the equation, particularly in light of the digital era. Furthermore, as both *Kolsuz* and *Touset* acknowledge, in the border context courts have only required reasonable suspicion for even the most intrusive nonroutine searches and seizures.[190] A requirement of reasonable suspicion therefore allows for a proper constitutional balance between the competing interests.[191]

On the privacy-side of the equation, due to the sheer amount of information stored on a cell phone or other electronic device, forensic searches are not necessarily carefully tailored to the border search's justifying principles.[192] Such a search might well uncover evidence of criminal wrongdoing, but it will also inevitably generate vast amounts of innocuous, sensitive information.[193] Based on *Touset*, if a customs official only held a bare-naked hunch that a certain traveler was in possession of child pornography or involved in trafficking narcotics, the official could forensically search that traveler's electronic devices. This search might reveal photos of child pornography, but it would also include details of the traveler's emails, messages, and Internet search history. And even

190. *See* United States v. Kolsuz, 890 F.3d 133, 147 (4th Cir. 2018) (citing United States v. Kolsuz, 185 F. Supp. 3d 843, 852-53 (E.D. Va. 2016)); *Touset*, 890 F.3d at 1233 (citing United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985)).

191. A pragmatic argument can be made that even if no level of suspicion is required for forensic searches, the majority of international travelers will likely be unaffected. CBP and ICE officials only have limited resources to conduct such searches and will therefore only act in instances where there is a real suspicion of criminal activity. Yet given the rapid pace of technological advances, one can imagine a near future where forensic searches can be conducted quite easily and efficiently. As noted in *Cotterman*, "[i]t is little comfort to assume that the government—for now—does not have the time or resources to seize and search the millions of devices that accompany the millions of travelers who cross our borders. It is the potential unfettered dragnet effect that is troublesome." United States v. Cotterman, 709 F.3d 952, 966 (9th Cir. 2013) (en banc).

192. *See*, Park, *supra* note 92 at 293.

193. It can also be argued that unlike physical contraband, digital contraband presents a more attenuated connection to the rationales underlying the border search exception. Digital contraband can also "cross" the border digitally, such as through the Internet. This argument was presented in *Alasaad* but was rejected by the court due to insufficient evidence in the record as to the claimed Internet transfers. No. 17-CV-11730-DJC, 2018 WL 2170323, at *19 (D. Mass. May 9, 2018).

though *Kolsuz*'s requirement of reasonable suspicion would not prohibit such a comprehensive search if reasonable suspicion exists, it would provide the appropriate safeguard for a traveler's Fourth Amendment rights.[194]

D. A "Reasonable Balance" at the Border Requires Reasonable Suspicion for All Searches of Electronic Devices

Even though *Touset* and *Kolsuz* only addressed the reasonableness of forensic searches of electronic devices, both opinions implicitly shed light on the issue of manual searches of such devices. Unlike pre-*Riley* cases such as *Cotterman*, the majority of *Touset*'s and *Kolsuz*'s discussion and reasoning surrounded electronic devices as a category, not merely the type of search performed. As courts continue to struggle with the proper treatment of searches of digital devices at the border, *Kolsuz* implicitly provides insight on how manual searches could and should be addressed in the near future.

The *Kolsuz* majority referred to the distinction between forensic and manual searches as "perfectly manageable,"[195] seeming to suggest a bright-line distinction between the two methods for purposes of the Fourth Amendment. However, several scholars have noted that post-*Riley*, such a distinction might be unwarranted.[196] While it is true that forensic searches inevitably involve a more intrusive process,[197] a manual search still implicates the same concerns expressed in *Riley* and *Kolsuz*. Although manual searches do not generate a "precise, comprehensive record" of the "uniquely sensitive" digital information,[198] the same

194. A plausible argument can be made that forensic searches should require at least probable cause, particularly given the nature of these searches. Government officials are not only able to access sensitive digitally stored information, but can access deleted files and efficiently sort through vast amounts of data. From a normative perspective, requiring probable cause is likely the desired outcome. However, searches at the border *are* fundamentally different given the context. And as even strip searches at the border only require reasonable suspicion, providing a greater constitutional protection for digitally stored information seems inappropriate.

195. United States v. Kolsuz, 890 F.3d 133, 146 (4th Cir. 2018) (citing *Cotterman*, 709 F.3d at 967).

196. *See, e.g.,* 5 LAFAVE, SEARCH & SEIZURE AT §10.5(F) (analyzing cases addressing the issue); Park, *supra* note 92 at 286-88 (although going on to argue that reasonable suspicion should be required); Laura Nowell, note, *Privacy at the Border: Applying the Border Search Exception to Digital Searches at the United States Border*, 71 FED. COMM. L.J. 85, 96-100 (2018) (arguing that courts should utilize the difference between forensic and manual digital searches as a factor in the analysis).

197. In *Arnold*, the Ninth Circuit held that CBP officers did not need reasonable suspicion to simply "boot . . . up" a laptop and manually search through the digital contents, as the search was not conducted in a "particularly offensive manner." 533 F.3d 1003, 1009-10 (9th Cir. 2008) In *Cotterman*, the court considered a forensic search of a laptop's hard drive. Given that *Arnold* only involved a "quick look and unintrusive search," the court distinguished *Arnold* on the ground that the forensic search was a comprehensive and "exhaustive exploratory search." 709 F.3d 952, 960-61, 966 (9th Cir. 2013).

198. *Kolsuz*, 890 F.3d at 145.

underlying information is still revealed to government officials through a manual search. The difference between a forensic and manual search is simply one of degree, and on a foundational level the information *Kolsuz* sought to protect from forensic searches is still implicated through manual searches.

Post-*Kolsuz,* it appears that such a distinction has the potential to, and should, be erased. For although *Kolsuz* addressed only forensic searches, much of the reasoning focuses on traveler's privacy interests in digital devices, rather than on the method of search.[199] The majority reads *Riley* as an express refusal to treat cell phones as "just another form of container," demonstrating *Riley*'s categorical basis for excluding cell phones from searches incident to arrest.[200] If courts do begin to rely on this categorization of cell phones and other electronic devices as being fundamentally different from traditional forms of tangible property, it is easy to see how manual searches could soon require reasonable suspicion. Given *Kolsuz*'s explicit recognition of the "uniquely sensitive nature" of digital information,[201] attempting to distinguish manual searches from forensic searches, such as a distinction between a search of a person and an x-ray or strip search, is illogical. Digital device searches are unique not merely because of the form of the search, but rather due to the information stored on the devices. Therefore, even a manual inspection still invokes the same privacy concerns associated with the more intrusive forensic search.

E. The Proper Role of the Courts

One nuance in the on-going judicial and scholarly debate is the question of a proper balance between the Judicial, Legislative, and Executive branches.[202] Essentially, the inquiry is whether courts should play an active role in deciding if some level of justification is needed to search digital devices at the border, or rather defer to the Legislative and Executive branches. This issue is particularly heightened in the context of electronic device searches at the border given the unique position of such searches. Digital device searches raise not only broader questions regarding how the Fourth Amendment applies to technological advances, but also a narrower question of how the former question changes when the search occurs at the border.

Touset represents a more cautious judicial approach, choosing to allow

199. *Id.* at 145-46.

200. *Id.* at 145.

201. *Id.*

202. *See, e.g.,* Kerr, *supra* note 48; Townsend, *supra* note 92 at 1745; Nadkarni, *supra* note 92 at 179-80.

Congress to develop the appropriate standard instead of "charging unnecessarily ahead."[203] The majority reasoned that the call for judicial caution is heightened in the sensitive context of border searches, as Congress is more capable of weighing the associated costs and benefits while developing new rules.[204] The concurring opinion in *Kolsuz* echoed this position, arguing for a separation of powers approach and criticizing the majority for wandering from the core role of the courts pursuant to Article III.[205] While this position has its merits, the historical premise of the Fourth Amendment and the reasonable expectation of privacy test of *Katz* suggests that courts should play an active role in regulating privacy when technological advances are involved.[206]

While a concern of separation of powers is somewhat implicated with digital device searches at the border, a judicial requirement of reasonable suspicion in no way oversteps the bounds of the Judiciary's constitutional responsibilities. Reasonable suspicion serves a fundamental role to balance the government's interests with an individual's privacy interest, merely establishing a constitutional baseline that customs officials cannot cross. This requirement simply protects travelers from unreasonable and unwarranted searches of their electronic devices; at a minimum, only those travelers whom customs officials have reasonable suspicion to believe are involved in criminal activity could have their electronic devices searched. The reasonable suspicion standard achieves the appropriate balance, ensuring law-abiding travelers need not worry about being subjected to an intrusive search of their electronic devices and sensitive digital information.

Although the Fourth Amendment establishes this baseline, Congress is still free to pass legislation requiring probable cause and/or a warrant for digital device searches at the border. Moreover, even though CBP recently issued a policy directive requiring reasonable suspicion for forensic searches of electronic devices,[207] this alone is inadequate. Such policy changes are encouraging, but only through judicial action, or legislation, can travelers be truly assured that they will not be subjected

203. United States v. Touset, 890 F.3d 1227, 1237 (11th Cir. 2018) (citing *Kolsuz*, 890 F.3d at 150 (Wilkinson, J., concurring in the judgment)). This position resonates with Orin Kerr's argument that when technology is in flux, courts should "place a thumb on the scale in favor of judicial caution . . . and consider allowing legislatures to provide the primary rules governing law enforcement investigation involving new technologies." Kerr, *The Fourth Amendment and New Technologies*, *supra* note 48 at 805.

204. Touset, 890 F.3d at 1237.

205. "The standard of reasonableness in the particular context of a border search should be principally a legislative question, not a judicial one." *Kolsuz*, 890 F.3d at 148 (Wilkinson, J., concurring in the judgment).

206. *See supra* Section II-B; *but see* Kerr, *supra* note 48 (arguing that courts should take a more cautious and conservative approach in favor of the legislative branch creating the primary investigative rules).

207. *See* U.S. CUSTOMS AND BORDER PROTECTION, DIRECTIVE NO. 3340-049A, *supra* note 9.

to a digital device searched without some level of suspicion justifying the privacy intrusion.

V. CONCLUSION

As of now, upholding suspicionless digital device searches at the border continues to be the norm among federal courts. The Fourth Amendment's border-search exception is generally interpreted as prohibiting a categorical distinction between electronic devices and traditional, tangible property, a distinction that pre-*Riley* had a proper precedential basis. Although post-*Riley* such a position can continue to be maintained, as demonstrated by *Touset*, this is the improper course. Cell phones and laptops by their very nature contain sensitive, personal information, and consequently searches of these devices invoke heightened privacy concerns. *Kolsuz* properly recognized this heightened interest, interpreting *Riley* as presenting a doctrinal change when analyzing searches of electronic devices under Fourth Amendment standards. And although *Kolsuz* distinguished between forensic and manual searches, such a distinction is likely to dissipate over time as both searches implicate individual privacy concerns of sensitive digital data. When balancing the traveler's interest against that of the Government in the international border context, reasonable suspicion provides the proper constitutional requirement for all searches of digital devices at the international border. Such a requirement ensures protection of individual liberty and privacy while still allowing Congress and the Executive branch ample room to regulate border searches, such as requiring a higher level of suspicion.