The Elephant in the Room: What Is a "Nonroutine" Border Search, Anyway? Digital Device Searches Post-*Riley*

by EUNICE PARK*

Introduction

Since the Supreme Court handed down *Riley v. California*[1] in 2014, we have been assured that if we are pulled over for speeding, the officer may not search our cell phone without a warrant. Another potential privacy peril, however, continues to loom: the international border. As the law currently stands, law enforcement agents may search our electronic devices, including cell phones and laptops, without any particularized suspicion, as we attempt to return into the United States from a trip abroad. Is this consistent with *Riley*? Or with the Fourth Amendment?

The wide latitude circuit courts have given government agents to conduct border searches has had a wrinkle since the 2013 *en banc* decision *United States v. Cotterman*, which deemed a forensic probe into the defendant's laptop "essentially a computer strip search."[2] In an 8-3 ruling, the Ninth Circuit held that agents must have "reasonable suspicion" before they can conduct a "thorough and detailed search of the most intimate details of one's life" contained within digital devices.[3] "[T]he uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy and thus renders an exhaustive exploratory search

* Associate Professor of Lawyering Skills, Western State College of Law. A special thank you to Western State College of Law Librarian Scott Frey for his invaluable research assistance; and Professors Robert Molko and Elizabeth Jones for their expertise and insights. The views expressed in this article are the author's own. I am grateful always to my parents, husband and children. I dedicate this article to my mom, Kyung S. Park, and to the memory of my dad, Jong M. Park.

1. Riley v. California, 134 S. Ct. 2473 (2014).
2. United States v. Cotterman, 709 F.3d 952, 966 (9th Cir. 2013).
3. *Id.* at 968.

more intrusive than with other forms of property."[4] *Cotterman* raises perhaps as many questions as it answers: what is an "exhaustive exploratory search?" Is it only a "forensic" examination? What is a "forensic" examination? Could a search that is less than "forensic" ever be considered "exhaustive" or "exploratory?" If so, at what point does the search cross the threshold from routine to nonroutine?

It was one year later that the Supreme Court produced its landmark decision in *Riley*, declaring that a warrant is required to search a cell phone, even one found on the person during a search incident to arrest.[5] Chief Justice Roberts explained that "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person" because of "their immense storage capacity."[6] Indeed, "many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."[7] Cell phones actually function as "minicomputers that also happen to have the capacity to be used as a telephone."[8] Moreover, the Court noted that cell phones also carry new kinds of data: browsing history, historical location information, and even information "located elsewhere," and that there is no way for officers to "know whether the information they are viewing was stored locally at the time of the arrest or has been pulled from the cloud."[9] For these reasons, the Court rejected the cell phone as container analogy.[10]

The Court also rejected the government's various "flawed proposals" for permitting warrantless cell phone searches under certain circumstances, such as allowing a warrantless search "whenever it is reasonable to believe that the phone contains evidence of the crime of arrest";[11] allowing a cell phone search of restricted areas of the phone;[12] allowing a search of a phone's call log;[13] or allowing a search of data that officers could have obtained from a pre-digital counterpart.[14] The Court pointed out that such an analogue test would allow law enforcement to search both a vast

4. *Id.* at 966.
5. *Riley*, 134 S. Ct. at 2473.
6. *Id.* at 2489.
7. *Id.* at 2490.
8. *Id.* at 2489.
9. *Id.* at 2491.
10. Riley v. California, 134 S. Ct. 2473, 2491 (2014).
11. *Id.* at 2491–92.
12. *Id.* at 2492.
13. *Id.* at 2492–93.
14. *Id.* at 2493.

quantity and vast array of information, and "would launch courts on a difficult line-drawing expedition . . . ."[15]

The Court acknowledged that its decision will impact the ability of law enforcement to combat crime; admittedly, "[p]rivacy comes at a cost."[16] However, the Court did leave the door ajar for warrantless searches where exigent circumstances arise under "some of the more extreme hypotheticals that have been suggested: a suspect texting an accomplice who, it is feared, is preparing to detonate a bomb, or a child abductor who may have information about the child's location on his cell phone."[17] What the Court found fundamentally concerning, however, was the immense privacy implications that warrantless cell phone searches would pose. Its answer "to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant."[18]

The U.S. Supreme Court denied the petition for writ of certiorari to have *Cotterman* heard along with *Riley*.[19] Yet, laptops are not just "minicomputers," but are actual computers and raise the same privacy concerns as cell phones, with an "immense storage capacity" just like cell phones. How might *Riley* impact border laptop searches? Moreover, how might *Riley* impact border searches of digital devices generally?

While other scholars have addressed this issue, this Article proposes a bright-line rule for border searches of laptops and other digital devices that resolves the problematic nature of the routine/nonroutine dichotomy by obviating it: All digital border searches, including laptops, should be subject to a reasonable suspicion standard without reference to whether the search is "routine" or "nonroutine." At the same time, in law enforcement's favor, this Article proposes that "border search" should not be tied to unmeaningful distinctions between inbound and outbound travelers, or imminent, versus ongoing, crime.

Part I of this Article describes the Fourth Amendment expectation of privacy and how that expectation is diminished at the border. Part II presents the history and precedent behind the routine versus nonroutine searches of laptops at the border, which leads to the Ninth Circuit split from other courts on the issue and some of the cases that have continued to develop the border laptop search issue since *Riley* and *Cotterman*. Part III provides a brief overview of the current literature that broadly can be

15. Riley v. California, 134 S. Ct. 2473, 2493 (2014).

16. *Id.*

17. *Id.* at 2494.

18. *Id.* at 2495.

19. United States v. Cotterman, 709 F.3d 952 (9th Cir.), *cert. denied*, 134 S. Ct. 899 (2014).

described as offering three major categories of approaches for border laptop searches: (1) reasonable suspicion should be required for all digital device searches; (2) reasonable suspicion should be required for some digital device searches; or (3) reasonable suspicion should never be required for digital device searches. Part IV proposes a straightforward alternative that follows the *Riley* example and the Supreme Court's expressed preference for "clear guidance to law enforcement through categorical rules"[20]: all digital border searches should be subject to a reasonable suspicion standard. This Article explains that the paradigm for digital searches should change by briefly addressing three precepts: (1) the privacy concerns implicated by *Riley* for searching "cell phones" apply to all digital devices; (2) an expectation of privacy still lives at the border for digital devices; and (3) case-by-case assessments are undesirable. This Article then offers an alternative that first, takes the elephant out of the room; second, maintains the balance between law enforcement and individual privacy by suggesting that this digital border search doctrine should apply equally to travelers exiting, as well as entering the United States, without being bound to pre-digital era notions of imminent, versus ongoing, crime.

I. The Fourth Amendment and the Diminished Expectation of Privacy at the Border[21]

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects" and mandates that a search or seizure conducted by a government agent must be "reasonable."[22] Although no general constitutional right to privacy exists and is not expressly written into the amendment's language,[23] Fourth Amendment jurisprudence encompasses an expectation of privacy.[24] The Fourth Amendment originally "was understood to embody a particular concern for government trespass,"[25] but since *Katz v. United States*, it also implicates a

20. *Id.* at 2491.

21. Portions of this passage are adapted from my article, Eunice Park, *Traffic Ticket Reasonable, Cell Phone Search Not: Applying the Search Incident-to-Arrest Exception to the Cell Phone as "Hybrid"*, 60 DRAKE L. REV. 429 (2012).

22. U.S. CONST. amend. IV.

23. *See* Katz v. United States, 389 U.S. 347, 350 (1967) ("[T]he Fourth Amendment cannot be translated into a general constitutional 'right to privacy.'"); *see also* Newhard v. Borders, 649 F. Supp. 2d 440, 449–50 (W.D. Va. 2009) ("[A]ny plausible claim would [not] arise . . . under privacy rights protected by the Constitution . . . .").

24. *See Katz*, 389 U.S. at 351 ("[T]he Fourth Amendment protects people, not places.").

25. United States v. Jones, 565 U.S. 400, 406 (2012).

reasonable expectation of privacy.[26] To invoke Fourth Amendment protection against unreasonable or warrantless searches based on a "*Katz* invasion of privacy,"[27] the area searched must be one in which there is a "constitutionally protected reasonable expectation of privacy."[28] This constitutionally protected reasonable expectation of privacy consists of both a subjective and objective requirement: "first[,] that a person have exhibited an actual (subjective) expectation of privacy, and second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[29]

Once this expectation of privacy is established, the burden is on the government to justify a warrantless search.[30] "[T]he Constitution requires 'that the deliberate, impartial judgment of a judicial officer . . . be interposed between the citizen and the police . . . .'"[31] A warrantless search is per se unreasonable, "subject only to a few specifically established and well-delineated exceptions."[32] Under the exceptions, certain types of searches and seizures are per se valid even in the absence of probable cause or a warrant.[33] The "border search" is one such exception.[34] The traditional tension under the Fourth Amendment between the interests of the Government and the privacy right of the individual generally favors the Government at the border.[35]

> The broad contours of the scope of searches at our international borders are rooted in the "long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country . . . ." Thus, border searches form "a narrow

26. *Id.* at 406–08; *but see id.* at 422 (Alito, J., concurring) (interpreting *Katz* as "finally [doing] away with the old approach, holding that a trespass was not required for a Fourth Amendment violation").

27. *Id.* at 408 n. 5.

28. *Katz*, 389 U.S. at 360 (Harlan, J.,concurring).

29. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see id.* at 352 (holding that a person in a telephone booth could rely upon the protection of the Fourth Amendment because "[o]ne who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world").

30. *Id.* at 357–59.

31. *Id.* at 357 (quoting Wong Sun v. United States, 371 U.S. 471, 481–82(1963)).

32. *Id.*

33. *See generally Katz*, 389 U.S. 347,357.

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

35. Almeida-Sanchez v. United States, 413 U.S. 266, 273 (1973) ("The needs of law enforcement stand in constant tension with the Constitution's protections of the individual against certain exercises of official power.").

> exception to the Fourth Amendment prohibition against warrantless searches without probable cause." Because "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border . . . border searches are generally deemed reasonable simply by virtue of the fact that they occur at the border."[36]

Two categories of border searches coexist: "routine" and "nonroutine."[37] A "routine" search of a person and his or her effects crossing an international border into the United States is not subject to any requirement of reasonable suspicion that an item contains contraband or evidence of criminal activity.[38] Border officials can conduct "routine" searches without any individualized suspicion.[39] On the other hand, a "nonroutine" search, involving a high degree of intrusion, such as a strip search, requires "reasonable suspicion," which is some particularized and objective basis for suspecting wrongdoing.[40] A "routine" search crosses the threshold and becomes "nonroutine" if the search is either particularly offensive, including an intrusive search of the body, or physically destructive.[41] Then, the presumption that most border searches do not require any suspicion of wrongdoing to be justified is rebutted.[42] Such a

36. United States v. Cotterman, 709 F.3d 952, 960 (9th Cir. 2013) (citing *Ramsey*, 431 U.S. at 616 (1977); United States v. Seljan, 547 F.3d 993, 999 (9th Cir. 2008); United States v. Flores-Montano, 541 U.S. 149, 152 (2004)).

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

38. *See generally* United States v. Ramsey, 431 U.S. 606 (1977) (regarding a customs inspection of mail).

39. *See Flores-Montano*, 541 U.S. at 152 (citing *Montoya de Hernandez*, 473 U.S. at 538).

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

41. United States v. Arnold, 533 F.3d 1003, 1007–08 (9th Cir. 2008); *cf.* YULE KIM, PROTECTING THE U.S. PERIMETER: BORDER SEARCHES UNDER THE FOURTH AMENDMENT 2 (2009) (similarly describing "(1) an intrusive search of the body, (2) a particularly destructive search of property, or (3) a search conducted in a particularly offensive manner").

42. KIM, *supra* note 41, at 2; *see* United States v. Seljan, 547 F.3d 993, 1003 (9th Cir. 2008) ("In *United States v. Ramos-Saenz*, 36 F.3d 59, 61 (9th Cir. 1994), we concluded that a border search goes beyond the routine 'only when it reaches the degree of intrusiveness present in a strip search or body cavity search' and that the search of the defendant's shoes in that case did not go beyond routine. In the context of vehicle searches, we have accepted the possibility that a search could conceivably be so destructive that it would exceed its reasonable scope, but have rejected arguments that the limit was exceeded in particular cases." (citations omitted)).

search is considered more invasive and requires a minimal showing of reasonable suspicion.[43]

II. Some Key Case Law Pre- and Post-*Cotterman* and *Riley*

Part II discusses how searches of laptops and other digital devices have been approached at the border. The cases will demonstrate that courts generally have been reluctant to grant defendants' motions to suppress evidence obtained from digital device border searches, holding that reasonable suspicion was present, whether or not it was required.[44] Since searches regularly have met the threshold for individualized suspicion for invasive searches, the courts generally have not pursued what makes a search routine or nonroutine.[45] Thus, the courts' proclivity traditionally has been to protect the Government's interests.[46] However, since *Cotterman* and *Riley*, courts are beginning to attempt to differentiate between routine and nonroutine searches and to exhibit concern when the search produces voluminous quantities of data.[47]

A. Pre-*Cotterman* and *Riley*

Courts did not always reach the question of whether reasonable suspicion was required where the search was supported by reasonable suspicion anyway.[48] The Fourth Circuit observed that computer searches, "[a]s a practical matter . . . are most likely to occur only where—as here—the traveler's conduct or the presence of other items in his possession suggest the need to search further."[49]

Even forensic analysis was permitted with little fanfare pre-*Cotterman*. In *United States v. Romm*, the court held that forensic analysis used by the U.S. Immigration and Custom Enforcement ("ICE") agents to

43. *See, e.g.*, United States v. Cotterman, 709 F.3d 952, 966 (9th Cir. 2013).

44. *See, e.g.*, United States v. Hassanshahi, 75 F. Supp. 3d 101, 118 (D.D.C. 2014).

45. KIM, *supra* note 41, at 17 ("[C]ourts have also been far more reticent in determining whether these types of searches are routine or non-routine. Instead, they have found that reasonable suspicion supported the searches, and, thus, they did not reach the question.").

46. See, e.g., United States v. Hassanshahi, 75 F. Supp. 3d 101, 118 (D.D.C. 2014).

47. *See generally* United States v. Kim, 103 F. Supp. 3d 32 (D.D.C. 2015); United States v. Djibo, 151 F. Supp. 3d 297 (E.D.N.Y.2015).

48. *See* KIM, *supra* note 41, at 17 ("Some lower federal courts . . . have held that searches of laptops and other forms of electronic storage devices fall under the border search exception.").

49. United States v. Ickes, 393 F.3d 501, 507 (4th Cir. 2005) (noting that customs official searched Defendant's van without a warrant near the Canadian border after noticing contents of van were inconsistent with Defendant's story of traveling on vacation; and the customs officials discovered, during a routine search, a videotape that focused excessively on a young ballboy during a tennis match and ultimately found childpornography).

recover deleted child pornography fell under the border search exception.[50] The court ultimately deemed the search routine and did not require probable cause, reasonable suspicion, or a warrant.[51] Yet the court went to lengths to describe the defendant's conduct, including his statement, "That's it. My life's over," and adopting a "confessional mode," even telling agents they had "every right to arrest him and would probably do so."[52]

Courts have not been swayed by defendants' argument that a computer contains highly private information and therefore should not be included under the umbrella of routine searches. One district court rebuked,

> [t]he Defendant would have this Court impute the same level of privacy and dignity afforded to the sovereignty of a person's being to an inanimate object like a computer. The Court finds this argument without merit. . . . [T]his Court cannot equate the search of a computer with the search of a person. The Court finds that the search of a computer is more analogous to the search of a vehicle and/or its contents.[53]

---

50. United States v. Romm, 455 F.3d 990, 997 (9th Cir. 2006).

51. *Id.* at 1006.

52. *Id.* at 994–95.

53. United States v. McAuley, 563 F. Supp. 2d 672, 677–78 (W.D. Tex. 2008) ("Incredible amounts of personal and sensitive information are already subject to scrutiny at ports of entry . . . . People carry personal items . . . [that] are already subject to routine border searches. A computer is simply an inanimate object made up of microprocessors and wires which happens to efficiently condense and digitize the information reflected . . . . The fact that a computer make take such personal information and digitize it does not alter the Court's analysis."); *see also, e.g.*, House v. Napolitano, No. 11–10852–DJC, 2012 WL 1038816, at *1 (D. Mass. Mar. 28 2012). Though this decision is unpublished, the district court's use of strong language in its holding that the digital search did not require reasonable suspicion is informative. House contended that a "search of a laptop and electronic devices implicates one's 'dignity and privacy interests,' not because there was any disrobing, physical search of his person, force used or exposure to pain or danger, but because such devices contain information concerning one's thoughts, ideas and communications and associations with others." *Id.* at *7. The court disagreed:

> [A] search of a laptop computer or other electronic devices does not involve the same "dignity and privacy interests" as the "highly intrusive searches of the person" found to require some level of suspicion such as strip searches or body cavity searches. *Flores–Montano,* 541 U.S. at 152. The Supreme Court has not explicitly held that all property searches are routine or that such searches are categorically incapable of implicating the "dignity and privacy interests of the person being searched," *id.,* but the search of one's personal information on a laptop computer, a container that stores

The Court noted further that "[a] search of items like a computer, unlike a strip search of a person, is not per se embarrassing."[54] In conclusion, the defendant's computer, hard drives, and any other belongings transported in his vehicle constituted "cargo," and the customs agents' searches of the computer and external hard drives at port of entry were routine border searches.[55]

United States v. Arnold similarly held that so long as a search is of a physical object rather than a person's body, reasonable suspicion is not required as long as the search is not physically destructive or particularly offensive.[56] The court held that a laptop is legally equivalent to property and a search does not intrude on a person's dignity and privacy interests to the same degree as a search of a traveler's body.[57] The characteristics that make electronic devices unique, including vast storage capacity and the ability to track its user's habits, tastes, and preferences, were determined to be not legally significant.[58] "Whatever 'particularly offensive manner' might mean, this search certainly does not meet that test."[59]

A case that has been a point of contrast to digital searches involved the overnight detention of a woman who eventually expelled eighty-eight balloons of cocaine while in custody. In *United States v. Montoya de Hernandez*, customs officials had a "reasonable suspicion" based on the suspect's inconsistent and implausible story that she was smuggling drugs in her alimentary canal.[60] The detention was "long, uncomfortable, indeed, humiliating," but supported by "the presence of articulable suspicion of

> information, even personal information, does not invade one's dignity and privacy in the same way as an involuntary x-ray, body cavity or strip search of person's body or the type of search that have been held to be non-routine and require the government to assert some level of suspicion.
>
> Rather, the search of House's laptop and electronic devices is more akin to the search of a suitcase and other closed containers holding personal information travelers carry with them when they cross the border which may be routinely inspected by customs and require no particularized suspicion.

Id.

54. *McAuley*, 563 F.Supp. 2d at 678.
55. *Id.* at 679.
56. United States v. Arnold, 533 F.3d 1003, 1007–10 (9th Cir. 2008).
57. *Id.* at 1008–09.
58. *Id.*
59. *Id.* at 1009.
60. United States v. Montoya de Hernandez, 473 U.S. 531, 531 (1985).

smuggling . . . ."[61] A recurring refrain has been that "a piece of property . . . simply does not implicate the same 'dignity and privacy' concerns as 'highly intrusive searches of the person.'"[62]

B. Post-*Cotterman* and *Riley*

Since *Cotterman* and *Riley*, courts have begun to exhibit self-consciousness of the lack of clarity on (1) whether or not reasonable suspicion is needed for digital device searches; and (2) if reasonable suspicion is needed, how to delineate the difference between routine and nonroutine searches.

1. Is Reasonable Suspicion Ever Needed?

One approach to the issue of whether reasonable suspicion is ever needed has been to deliberately avoid it. In *United States v. Hassanshahi,* law enforcement agents were alerted that Hassanshahi, a suspect involved in a prior federal law enforcement investigation into potential violations of the Iran trade embargo, would be returning to the United States the next day through the Los Angeles International Airport.[63] He was referred to secondary screening and law enforcement conducted a forensic search of his laptop.[64] The court stated, "because the Court ultimately concludes that there was reasonable suspicion for the forensic examination of Hassanshahi's laptop, the constitutional question of whether that examination required reasonable suspicion becomes moot."[65] Additionally, the court included a lengthy footnote distinguishing its approach from that of the courts in *Cotterman* and *United States v. Saboonchi*, both of which "found reasonable suspicion for the respective forensic computer examinations, yet . . . spent considerable space addressing a constitutional question that had no practical effect on the final disposition of the case."[66] By contrast, the *Hassanshahi* Court found "that engaging in such an

61. *Id.* at 544.

62. United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008) (citing United States v. Flores-Montano, 541 U.S. 149, 152 (2004)).

63. United States v. Hassanshahi, 75 F. Supp. 3d 101, 105 (D.D.C. 2014); *see* United States v. Saboonchi, 990 F. Supp. 2d 536 (D. Md. 2014) (holding that warrantless forensic search of cell phone and flash drive at border was supported by reasonable suspicion). See cases cited in *Saboonchi*, 990 F. Supp. 2d at 560.

64. *Hassanshahi*, 75 F. Supp. 3d at 106–07.

65. *Id.* at 119.

66. *Id.* at 119 n.11.

exercise would be imprudent unless reasonable suspicion was found not to exist."[67]

Other courts note that the reasonable suspicion requirement is unresolved and go on to reject the notion that a laptop search, even a forensic one, requires any particularized suspicion at all, echoing some of the pre-*Cotterman* decisions. For example, in *United States v. Feiten,* the district court held that "[a]llowing customs officials without a warrant to forensically search an electronic device presented at an international border or its equivalent is utterly consistent with its historical mooring of protecting the country by preventing unwanted goods from crossing the border into the country."[68] Even if any level of suspicion was required, it would only be reasonable suspicion.[69]

> Even if the court were to find that making "a full digital copy [of] the computer's hard drive" and testing it was considered a highly intrusive search that infringed on Defendant's "dignity and privacy interests," . . . — although the court is not at all convinced that it was— Defendant has failed to point to any authority suggesting that such a conclusion would necessitate a warrant. To the contrary, the Supreme Court and Sixth Circuit have both indicated that even the highly intrusive searches that are carried out in a "particularly offensive manner" such as "strip searches or body cavity searches" require only that the border agents to have reasonable suspicion [sic].[70]

The court outright dismissed concerns expressed in *Riley* about searching digital technology: "Laptops and cell phones are indeed becoming quantitatively, and perhaps qualitatively, different from other

67. *Id.* See generally cases cited in *Saboonchi*, 990 F. Supp. 2d at 560. *See also* United States v. Wallace, No. 1:12–CR–230–1–TWT, 2013 WL 1702791, at *1 (N.D. Ga. Apr. 19, 2013); United States v. Martinez, No. 13CR3560–WQH, 2014 WL 3671271, at *1 (S.D. Cal. July 22, 2014); United States v. Molina-Gomez, 781 F.3d 13, 19–20 (1st Cir. 2015); United States v. Kim, 103 F. Supp. 3d 32, 53 (D.D.C. 2015); United States v. Blue, No. 1–14–CR–244–SCJ, 2015 WL 1519159, at *2 (N.D. Ga. Apr. 1, 2015) ("It is not necessary, however, to determine whether the intrusion into the cell phone would require a higher standard of justification than merely Defendant's presence at the border. Here, . . . it is beyond cavil (and, indeed, beyond peradventure as well) that the officers had reasonable grounds . . . to suspect that evidence of drug importation would likely be found on Defendant's . . . cell phone.").

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

69. *Id.* at *7.

70. *Id.* (internal references and citations omitted).

items, but that simply means there is more room to hide digital contraband, and therefore more storage space that must be searched."[71]

2. *If Reasonable Suspicion Is Needed, in What Kinds of Searches?*

For those courts that have begun to consider the difference between routine and nonroutine searches and have ventured to resolve that a nonroutine search requires reasonable suspicion, while a routine search does not, the terms to distinguish the two searches are vague and the analysis seems strained.

One district court attempted to distinguish between routine and nonroutine searches by differentiating between a "quick look" and an "exhaustive search."[72] In *Abidor v. Napolitano*, the court held that border agents had reasonable suspicion, supporting further inspection of a graduate student's electronic devices and describing a "quick look" as "only a cursory search that an officer may perform manually. It involves opening the computer and viewing the computer's contents as any lay person might be capable of doing simply by clicking through various folders."[73] A forensic examination, in contrast, "involves an exhaustive search of a computer's entire hard drive," including "a hard drive's unallocated space."[74] The district court in *United States v. Caballero* likewise agreed that a "cursory" search of a cell phone, without reasonable suspicion, is permissible at the border.[75]

One month after *Caballero*, in *United States v. Kolsuz*, a district court in Virginia observed that "the line between routine and nonroutine border searches remains somewhat indistinct," but determined that "the juxtaposition of the two searches of defendant's iPhone well-illustrates where the dividing line exists with respect to the border searches of electronic devices."[76] The court held that the first search, a "manual inspection of text messages and recent calls on defendant's iPhone," was a routine search.[77] On the other hand, an off-site forensic search was a nonroutine border search that must be supported by particularized

71. *Id.* at *6; *see* United States v. Dattmore, No. 12–CR–166A, 2013 WL 4718614 at *4 (W.D.N.Y. Sept. 3, 2013) (suggesting that a search of a computers and electronic devices is akin to searching luggage or personal belongings traditionally considered routine searches and likewise do not require reasonable suspicion); United States v. Thompson, 53 F. Supp. 3d 919, 922–23 (W.D. La. 2014).

72. Abidor v. Napolitano, 990 F. Supp. 2d 260, 269–70 (E.D.N.Y. 2013).

73. *Id.* at 269–70.

74. *Id.* (citing United States v. Cotterman, 709 F.3d 952, 960 (9th Cir. 2013)).

75. United States v. Caballero, 178 F. Supp. 3d 1008, 1016 (S.D. Cal. 2016).

76. United States v. Kolsuz, 185 F. Supp. 3d 843, 854 (E.D. Va. 2016).

77. *Id.* at 854–55 (citing United States v. Ickes, 393 F.3d 501, 505–06 (4th Cir. 2005)).

suspicion.[78] Seeming to grasp for a frame of reference, the court noted that the second, forensic search "was not as extensive as the forensic search in *Saboonchi*, to be sure," but ultimately concluded that the search "nonetheless implicated significant privacy interests. To suggest otherwise is like suggesting that a strip search does not implicate a significant privacy interest so long as the government does not look between the person's toes."[79] Accordingly, "although the Supreme Court's decision in *Riley* appears to indicate that cell phones deserve the highest level of Fourth Amendment protection available, the highest protection available for a border search is reasonable suspicion."[80] Thus, "a nonroutine border search of a cell phone is constitutional if it is supported by reasonable suspicion."[81]

Another district court seemed to define a conventional search largely by the amount of time, as a practical matter, that a customs officer can spend.[82] In *United States v. Saboonchi,* the court explained:

> [A] conventional search is limited by the amount of time one [c]ustoms officer has to devote to reviewing the contents of digital evidence at the border . . . . [T]he amount of data searched will be a mere fraction of what is on the device, given the storage capacity of modern electronic devices.[83]

78. *Kolsuz*, 185 F. Supp. 3d at 858.

79. *Id.* at 857 (referencing United States v. Saboonchi, 990 F. Supp. 2d 536, 539–40 (D. Md. 2014)). Defendant's digital devices were seized at the border, imaged, and thereafter forensically searched using specialized software.

80. *Kolsuz*, 185 F. Supp. 3d at 858–59.

81. *Id.* at 859.

82. *Saboonchi*, 990 F. Supp. 2d at 547.

83. *Id.* A "conventional inspection of electronic media and a review of the files on them" is routine, because it is akin to reviewing physical papers. *Id.* at 552. In contrast, a forensic examination is distinguished by the use of "sophisticated technology-assisted search methodologies [that] can exceed vastly the capacity of a human searching and viewing files. Moreover, this type of search exposes a class of data that raises novel privacy concerns, including files that a user had marked as 'deleted' and location data that may provide information about activities in the home and away from the border." *Id.* at 547–48. Accordingly, forensic searches may be conducted if a Customs officer has a reasonable, particularized suspicion that a particular device contains contraband or evidence of criminal activity. *Id.* at 570. Following the April 2014 decision, Defendant moved for reconsideration in light of the June 2014 *Riley* decision. United States v. Saboonchi, 48 F. Supp. 3d 815, 816 (D. Md. 2014). In July 2014, the district court denied Defendant's motion for reconsideration, finding that Riley "involved conventional searches, not forensic searches . . . ." *Id.* at 819. Accordingly, "[a]n invasive and warrantless border search may occur on no more than reasonable suspicion . . . ." *Id.*

Border searches producing large quantities of data have triggered similar concerns. For example, in *United States v. Kim*, the court held that the pre-planned warrantless search of the laptop computer, seized before the defendant boarded the plane, "was supported by so little suspicion of ongoing or imminent criminal activity, and was so invasive of [defendant's] privacy," that it violated the Fourth Amendment.[84] The court was concerned that agents had asked for and obtained a warrant but conducted no further search because they had already obtained all the information from the initial search.[85] The defendant's hard drive had been copied so it could be searched for an indefinite duration using specialized software, and the examination occurred for weeks at a location other than the border.[86] The Court described the search of Kim's laptop as falling "somewhere on the spectrum between the two poles [of forensic and non-forensic searches] described by other courts."[87] Indeed, the Court pointedly noted that "the forensic specialist . . . acknowledged that the term 'forensic search' can describe a range of examinations and that the term has no specific definition."[88] Ultimately the court concluded that the search was "nothing more than a fishing expedition to discover what Kim might have been up to."[89] Echoing *Riley*, the court deemed it inappropriate to simply categorize the laptop as a "container" to assess the search's reasonableness.[90] In fact, "while the immediate national security concerns were somewhat attenuated, the invasion of privacy was substantial," leading the Court to "ask itself whether the examination in this case can accurately be characterized as a border search at all."[91]

A "921 page 'peek'" into a cell phone at the border was similarly found to be objectionable.[92] In *United States v. Djibo*, the defendant was stopped before the actual jet way and found to be carrying "a number of

84. United States v. Kim, 103 F. Supp. 3d 32, 59 (D.D.C. 2015).

85. *Id.*

86. *Id.* at 57.

87. *Id.* at 52. Ultimately the court was forced to turn to the traditional weighing of intrusion of privacy against protecting legitimate government interests. *Id.* at 55.

88. *Id.* at 52.

89. United States v. Kim, 103 F. Supp. 3d 32, 46 (D.D.C. 2015).

90. *Id.* at 55; *cf.* United States v. Molina-Gomez, 781 F.3d 13, 17, 19–20 (1st Cir. 2015) (holding that even assuming the search a search of physical space in the hardware of a computer disassembled by agents, where bags of heroin were found hidden inside, was non-routine, reasonable suspicion existed to justify the search). *See* United States v. Lara, 815 F.3d 605, 610–11 (9th Cir. 2016) (distinguishing between property as physical objects that can be possessed, versus data, which is information that "not only cannot be possessed physically; it is also not 'under [Lara's] control'").

91. *Kim*, 103 F. Supp. 3d at 56–57.

92. United States v. Djibo, 151 F. Supp. 3d 297, 309 (E.D.N.Y. 2015).

cellular phones."[93] After he was arrested and Mirandized, law enforcement agents "ran an initial Cellebrite report or an initial search on the phone, *just a preliminary peek.*"[94] When the "Court requested a copy of what the government called a 'peek,' . . . the government surprisingly revealed that the report would be voluminous."[95] Eventually the government asked the court "to find that the warrantless 'peek' into his phone is suppressible, but not the thousands of pages retrieved through a subsequent forensic search" obtained via warrant.[96] The court held that the search was unreasonable since the search warrant relied on the "poisonous 'peek'" and any information obtained was fruit of the illegal initial search of the phone.[97] Although the case holding hinges on technicality of the defendant not being Mirandized, the court was concerned with the nature of the "poisonous peek," pointedly noting,

> [A]s the *Riley* court held, a cell phone is not just a physical object containing information. It is more personal than a purse or a wallet . . . . It is the combined footprint of what has been occurring socially, economically, personally, psychologically, spiritually and sometimes even sexually, in the owner's life, and it pinpoints the whereabouts of the owner over time with greater precision than any tool heretofore used by law enforcement without aid of a warrant. In today's modern world, a cell phone passcode is the proverbial "key to a man's kingdom."[98]

Thus, the current status of the case law is well captured by the *Kolsuz* court:

> Although the Supreme Court has not made pellucid exactly what renders a border search nonroutine—and what level of individualized suspicion is necessary for nonroutine searches—circuit courts have looked to the intrusiveness of the search in distinguishing between routine and

93. *Id.* at 299.

94. *Id.* at 302 (citing law enforcement agent's testimony in transcript).

95. *Id.* at 303.

96. *Id.* at 307–08.

97. United States v. Djibo, 151 F. Supp. 3d 297, 309–10 (E.D.N.Y. 2015).

98. *Id.* at 310; *see* United States v. Cano, No. 16–cr–01770–BTM, 2016 WL 6920449, at *5 (D. Az. Nov. 23, 2016) (holding that the Cellebrite search was lawful since the border agents had reasonable suspicion that evidence of narcotics trafficking may exist on the cell phone).

> nonroutine border searches. . . . Less clear, however, is whether digital searches of electronic devices—such as computers and cell phones—count as routine border searches.[99]

The following section summarizes some of the efforts to reconcile the law and offer solutions.

III. Controversy in the Current Literature

For some, the focus is to pose the essential question: whether the "significant impact on privacy interests recognized in *Riley* will be sufficient to require a showing of individualized suspicion for border searches of digitally stored information."[100] Others take a stance that can be described as generally falling into one of three camps: (1) reasonable suspicion should be required for all digital device searches at the border; (2) reasonable suspicion should be required for some digital device searches at the border; or (3) reasonable suspicion is never required for digital device searches at the border. All of these scenarios, however, leave unresolved the elephant in the room: what is the difference between a routine and nonroutine search, anyway?

A. Reasonable Suspicion Should Be Required for All Digital Device Border Searches

Some scholars urging reasonable suspicion for all digital searches focus on privacy, the particularity of the search, and the metaphysical nature of digital data.

---

99. United States v. Kolsuz, 185 F. Supp. 3d 843, 853 (E.D. Va. May 5, 2016).

100. Andrew Pincus, *Evolving Technology and the Fourth Amendment: The Implications of* Riley v. California, 2014 CATO SUP. CT. REV. 307, 336 (2014); *see* Jordi de la Torre, *Development in the Judicial Branch: The Ninth Circuit Holds that a Forensic Examination of a Laptop at the Border Requires Reasonable Suspicion*, 28 GEO. IMMIGR. L.J. 507, 513–14 (2014) ("If another federal court of appeals [in addition to the Ninth Circuit] or a state's highest court in the future upholds a suspicionless forensic examination of electronic devices at the border, the Supreme Court is likely to intervene in order to settle the question."); *see also, e.g.*, Jody Thomas López-Jacobs, *Is There a Border Exception to the Exclusionary Rule?*, 87 TEMP. L. REV. 611, 643 (2015) (stating that enforcing the exclusionary rule at the border "will incentivize border officials to continue conducting searches under existing Fourth Amendment limitations. . . . [and] refrain from conducting invasive, nonroutine searches (such as strip searches and x-ray searches) unless they have reasonable suspicion of criminal activity." This, in turn, "will ensure that courts continue to debate Fourth Amendment issues, such as whether the forensic search of Howard Cotterman's laptop is constitutional—with or without reasonable suspicion of illegal activity . . . and that one's Fourth Amendment rights are not virtually forfeited by merely crossing an international line.").

One author posits that "[t]he central question . . . is whether searches of electronic devices are seen as more like strip searches or more like pat-downs."[101] Summing up the results of a survey, the author found that "[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."[102] Thus, the article urges, "[i]mposing a reasonable suspicion standard for searches of electronic devices would be a fairly modest step given the strength of the privacy interests implicated," which, based on the study, "are very powerful. They are more powerful, in fact, than some courts have presumed."[103]

Another scholar's concern with privacy leads to a focus on ensuring "particularity" in computer searches: "the means by which a search is 'carefully tailored to its justifications' and does not become a general exploratory search."[104] Digital searches are especially concerning, since "large amounts of data—some relevant to the investigation, but much of it likely irrelevant—are stored on a computer, cellphone or email account."[105] Based on these concerns, the author lauds *Riley* for providing "support to lower courts considering whether to adopt *Cotterman*'s reasonable suspicion requirement for intensive electronic searches at the border, and suggests even a simple cursory look through a phone at the border may be constitutionally problematic."[106]

> Just as rifling through all of the data on a phone goes beyond the *Chimel* justifications for the search incident to arrest exception, a search of an electronic device—allowing government access into reams of digital data—is more invasive than necessary to monitor what comes in and out of the border, particularly when so much data is

101. Matthew B. Kugler, *The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study*, 81 U. CHI. L. REV. 1165, 1177 (2014) (referring to *United States v. Montoya de Hernandez*, in which the Court held that reasonable suspicion was required for the nonroutine search of contents expelled from Defendant's alimentary canal after overnight detention; and *Flores-Montano*, in which the Court held that no reasonable suspicion is necessary to search a gas tank, which is a routine search that imputes no privacy interests).

102. *Id.* at 1211.

103. Id.

104. Hanni M. Fakhoury, *Digital Searches After* Riley v. California, 39-MAR Champion 36, 39 (2015) (quoting Maryland v. Garrison, 480 U.S. 79, 84(1987)).

105. Fakhoury, *supra* note 104, at 39.

106. Id.

> stored remotely in the cloud rather than on the electronic device directly.[107]

Finally, the concept of remote storage overlaps with the approach of those who view the issue as raising a question of physical intangibility. While a gas tank is

> strictly "property" in the classical sense, in that it does not . . . assume or take upon itself the personhood of its owner . . . . clearly such a piece of property as a laptop or smart phone possesses a greater measure of personhood than a gas tank, if anything for the digital device's ability to embody and transmit the person's thoughts and expressions.[108]

Along with "personhood," the digital device's contents are intangible and "strikes the traveler as removed from the scope and ambit of the search."[109] Unlike a traditional physical search of a "container" that stores files, searching a laptop or digital device provides "access to a digital realm that is removed from any physical spatio-temporal location . . . ."[110] The author thus compares a digital search to an "extended border search," and concludes that, "all border searches of digital devices," not just those where the device is detained for a prolonged period or when a forensic analysis is conducted, necessitate reasonable suspicion.[111]

B. Reasonable Suspicion or Probable Cause Should Be Required for Certain Kinds of Digital Device Border Searches, and Legislation May (or May Not) be the Solution

Many others narrow the reasonable suspicion requirement to apply only to certain kinds of searches at the border, alternatively defined as

---

107. Id.

108. Tom Rechtin, *Back to the Future of Your Laptop: How Backlash Over Prolonged Detention of Digital Devices in Border Searches Is Symptomatic of a Need for "Reasonable Suspicion" in All Border Searches of Digital Devices*, 7 THE CRIT: CRITICAL STUD. J. 66, 87 (2014).

109. *Id.* at 88; *see* Victoria Wilson, *Laptops and the Border Search Exception to the Fourth Amendment: Protecting the United States Borders From Bombs, Drugs, and the Pictures From Your Vacation*, 65 U. MIAMI L. REV. 999, 1019 (2011) ("The authority to open a laptop to search for physical objects without suspicion should not extend to the information contained within the laptop.").

110. Rechtin, *supra* note 108, at 89.

111. *Id.* at 89–90.

"forensic," "nonroutine," "exhaustive," "intrusive," or "intensive," with many using one or more of these terms interchangeably.[112]

"[T]here are times when the government must realize that the nature of certain types of searches goes too far when weighed against an individual's privacy interests."[113] While maintaining that national security is paramount, "an 'exhaustive forensic search of a copied laptop hard drive,'" urges the author, "is one of those times . . . [because it] 'intrudes upon privacy and dignity interests to a far greater degree than a cursory search at the border.'"[114]

In fact, "[g]iven the Supreme Court's conclusion that digital searches can be more intrusive than the search of a home, and are fundamentally different from searches of a person or physical property," another author questions whether the border search exception should apply to digital searches at all.[115] Assuming that some sort of border exception exists, the author urges that digital searches should require reasonable suspicion or even probable cause.[116] "[C]ourts should treat digital searches as nonroutine . . . and [do] away with the distinction between manual and forensic searches."[117] Indeed, "*Riley*'s recognition of the unique intrusiveness of a digital search supports a probable cause standard."[118]

In contrast, another view "reject[s] the argument that the large storage capacity of laptops and their capability to store personal information makes laptops completely distinct from any nondigital object,"[119] and advocates for viewing personal digital device border searches instead as "a close relative of special needs searches."[120] The author calls for a simplified application of the conventional special needs balancing test to digital

112. *See, e.g.*, *infra* at notes 113–28; *cf* Ari B. Fontecchio, *Suspicionless Laptop Searches Under the Border Search Doctrine: The Fourth Amendment Exception that Swallows Your Laptop*, 31 CARDOZO L. REV. 231, 236 (2009) ("[T]he government should require a customs agent to have 'one good reason' before performing an intrusive data search at the border. This standard would require an officer to have more than no suspicion yet less than a reasonable suspicion or probable cause to search the data inside one's laptop.").

113. Ryne Spengler, *Hijacked at the Border: Why the Government Should Have Reasonable Suspicion Before Conducting Intrusive Examinations of Our Personal Electronic Devices*, 11 SETON HALL CIR. REV. 431, 452(2015).

114. *Id.* at 452 (citing United States v. Cotterman, 709 F.3d 951, 966 (9th Cir. 2013)).

115. Thomas Mann Miller, *Digital Border Searches After* Riley v. California, 90 WASH. L. REV. 1943, 1995(2015).

116. Id.

117. Id.

118. *Id.* at 1995–96.

119. Sid Nadkarni, *"Let's Have a Look, Shall We?" A Model for Evaluating Suspicionless Border Searches of Portable Electronic Devices*, 61 UCLA L. REV. 146, 152 (2013).

120. *Id.* at 151.

border searches, and to determine intrusiveness by considering factors relevant in other special needs cases.[121] However, "searches that are nonforensic and that reveal minimal information to human observation would be more likely to be permissible without any level of suspicion."[122]

Requiring anything less than probable cause, however, raises another concern.[123] "[F]orward-thinking federal agents"[124] may consider the border search exception as a warrant loophole where, lacking probable cause, law enforcement officers "could wait for their suspect to arrive at the border and then have customs officials search the suspect's digital devices based only on reasonable suspicion—or no suspicion at all for a conventional search."[125] Since "*Riley* does not foreclose warrantless searches of electronics at the border,"[126] the author explains that "the government can use the [border search] exception to skirt traditional Fourth Amendment protections."[127] The author concludes that "more intensive searches" of electronic devices should require reasonable suspicion.[128]

The suggestion of a legislative approach for suspicionless border searches raises controversy as well. One position is that the simultaneous importance of the government's interests and the significant individual privacy concerns posed by the border search exception for electronic searches, in conjunction with the current state of the law, makes the Supreme Court "highly unlikely to provide a judicial remedy requiring heightened suspicion for forensic computer searches."[129] Thus, the likely solution is through the legislative process.[130]

---

121. *Id.* at 153–54 (Other relevant factors include "the nature and amount of the information searched, the duration of the search, and the presence or absence of an extended detention of the property.").

122. *Id.* at 188.

123. Jared Janes, *The Border Search Doctrine in the Digital Age: Implications of* Riley v. California *on Border Law Enforcement's Authority for Warrantless Searches of Electronic Devices*, 35 REV. LITIG. 71, 102 (2016).

124. *Id.* at 99.

125. *Id.* at 102.

126. *Id.* at 99.

127. *Id.* at 101. As an example, the author cites *United States v. Saboonchi*, 990 F. Supp. 2d 536 (D. Md. 2014), in which, by deliberately placing Saboonchi on the travel watch list, agents were able to be alerted as soon as he traveled internationally, providing the opportunity to search his electronics, though his crime, trade violations with Iran, "had nothing to do with his presence at the border." *Id.* at 99.

128. *Id.* at 75, 99.

129. Samuel A. Townsend, *Laptop Searches at the Border and* United States v. Cotterman, 94 B.U. L. REV. 1745, 1779 (2014).

130. Id.

In contrast stands the position that legislation requiring individualized suspicion for intrusive digital devices is unlikely, based on the "failures of recent Congressional efforts to curb digital border searches . . . ."[131] Instead, "[b]ecause the executive and legislative branches have proved unwilling and unable to subject any type of digital border search to a reasonable suspicion standard, reform is most likely to come from the judiciary."[132]

Thus, even among those who favor some form of reasonable suspicion, controversy is rife.

C. No Reasonable Suspicion Is Required for Digital Device Border Searches

At the other end of the spectrum is the position that no particularized suspicion is ever required for any digital border searches. One reason for this view is that requiring reasonable suspicion for forensic examinations is administratively impractical and would impede law enforcement agents' ability to protect national security.[133] This argument urges a return to the container analogy and that all forms of property should be treated the same, regardless of storage capacity:

> Suitcases, luggage, and any other traditional storage containers are always subjected to suspicionless border searches even if they contain large amounts of personal information. Merely converting the personal information contained in a suitcase into an electronic form should not be enough to bestow heightened constitutional protection.[134]

Furthermore, since border agents "have the ability to copy data from confiscated hard drives to government-owned devices[, t]his data can then be shared with a variety of government agencies or even retained for an indefinite period of time without ever alerting travelers."[135] The solution "to prevent the misuse of this sensitive information," the author posits, is to implement agency regulations, and grant travelers the right to sue Customs

131. Nadkarni, *supra* note 119, at 179.

132. *Id.* at 180.

133. Michael Creta, *A Step in the Wrong Direction: The Ninth Circuit Requires Reasonable Suspicion for Forensic Examinations of Electronic Storage Devices During Border Searches in* United States v. Cotterman, 55 B.C. L. REV. E. SUPPLEMENT 31, 40–45 (2014).

134. *Id.* at 41.

135. *Id.* at 43–44.

and Border Patrol or Immigration and Customs Enforcement "for directive violations."[136]

The controversy in the current literature demonstrates a need for clarity and closure on the issue of digital device border searches.

IV. Proposal: Application to Digital Device Searches at the Border

This Article approaches the solution of a reasonable suspicion standard for all digital devices without hinging analysis on the routine/nonroutine paradigm. This section discusses why the paradigm should change, first, by briefly addressing three fundamental precepts. Next, this section proposes an alternative that takes the elephant out of the room and considers both inbound and outbound travelers and what "reason to suspect that criminal activity [is] afoot" should encompass.[137]

A. Why the Paradigm Should Change

First, the privacy concerns implicated by *Riley* for cell phones apply equally to all digital devices. Despite *Riley*'s clear directive that cell phones, as a digital device, are different in both a "quantitative and qualitative sense" from other objects that were the traditional object of searches,[138] some courts have been reluctant to abandon the digital device as container model.[139] *Riley* also established that a cell phone is much more than a phone. The "term 'cell phone' is itself misleading shorthand; many of these devices are in fact *minicomputers* that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[140] Thus, the privacy implications for searching "cell phones" applies to all digital devices,

136. *Id.* at 44–45.

137. *See, e.g.*, United States v. Kim, 103 F. Supp. 3d 32, 35 (D.D.C. 2015).

138. Riley v. California, 134 S. Ct 2473, 2489 (2014).

139. *See, e.g.*, *supra* at note 71.

140. *Riley*, 134 S. Ct. at 2489 (emphasis added); *see* United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013), *petition for cert. filed*, Petition for Writ of Certiorari, *Cotterman*, 2014 WL 491626, at *3 (2014) (No. 13-186) ("Although [*Riley* and *Wurie*] involved telephones rather than laptop computers, that distinction is no longer important, having diminished over the years as the functions of those devices merge. Personal electronic devices of all shapes and sizes now commonly have internet connectivity, search capability, and the capacity to hold a lifetime of highly personal information, including photos and videos.").

particularly of the "mini" variety that a traveler is likely to be carrying at the border.[141]

Second, recognizing that the privacy implications for cell phones, laptops, or other digital devices are indistinguishable, the next issue is whether an expectation of privacy is maintained for digital devices at the border. The answer is yes.

Searches at the border that are physically destructive or particularly offensive have been subject to a reasonable suspicion standard.[142] While a search of the digital contents of a device does not raise the specter of physical destruction, it does raise the specter of being particularly offensive. A search is "particularly offensive" if it is highly intrusive into the dignity and privacy interest of the person searched.[143] It has been suggested that the category of "particularly offensive" should be limited to searches of a person such as strip searches, body cavity searches, and involuntary x-ray searches.[144] This notion, however, relies on the traditional model of physical items as mere containers that *Riley* has made obsolete, and disregards what *Riley* called the quantitatively and qualitatively unique characteristics of digital devices.[145] An attempt to impose such a limitation has already been outright rejected. In *Kim*, the government attempted to argue that the search of defendant's laptop "was not physically invasive or embarrassing and not even destructive of the laptop itself, which was returned to the defendant intact."[146] The court refuted this approach, describing it as "the task of applying eighteenth-century principles to this twenty-first-century technology."[147]

> [G]iven the vast storage capacity of even the most basic laptops, and the capacity of computers to retain metadata and even deleted material, one cannot treat an electronic

141. *See, e.g.*, United States v. Saboonchi, 990 F. Supp. 2d 536 (D. Md. 2014) (concerning smart phones and a flash drive); United States v. Lara, 815 F.3d 605 (9th Cir. 2016) (regarding cell phones); United States v. Molina-Gomez, 781 F.3d 13 (1st Cir. 2015) (involving a laptop and electronic gaming system).

142. United States v. Arnold, 533 F.3d 1003 (9th Cir. 2008); *see* KIM, *supra* note 41, at 2.

143. United States v. Montoya de Hernandez, 473 U.S. 531, 540 n.3 (1985).

144. *Id.* at 541 n.4; *see* United States v. Feiten, No. 15-20631, 2016 WL 894452, at *7 (E.D. Mich. Mar. 9, 2016); House v. Napolitano, No. 11–10852–DJC, 2012 WL 1038816, at *7 (D. Mass. Mar. 28 2012); *see also supra* notes 68–70.

145. *See, e.g.*, David D. Cole, *After Snowden: Regulating Technology-Aided Surveillance in the Digital Age*, 44 CAP. U. L. REV. 677, 679–80 (2016).

146. United States v. Kim, 103 F. Supp. 3d 32, 50 (D.D.C. 2015).

147. *Id.* at 51.

> storage device like a handbag simply because you can put things in it and then carry it onto a plane.[148]

The district court in *Arnold* similarly held that the government's border search of the information on the defendant's electronic storage devices violated the Fourth Amendment:

> Fourth Amendment protection extends to the search of this type of personal and private information at the border. While not physically intrusive as is the case of a strip or body cavity search, the search of one's private and valuable personal information stored on a hard drive or other electronic storage device can be just as much, if not more, of an intrusion into the dignity and privacy interests of a person. This is because electronic storage devices function as an extension of our own memory. They are capable of storing our thoughts, ranging from the most whimsical to the most profound. Therefore, government intrusions into the mind—specifically those that would cause fear or apprehension in a reasonable person—are no less deserving of Fourth Amendment scrutiny than intrusions that are physical in nature.[149]

Although the district court was reversed on appeal, the court's observations recognize the shortsightedness of limiting intrusions considered particularly offensive merely to the physical realm. In the modern digital age, reality is much more layered and complex. Use of the cell phone, or other digital items, has become an integral part of multiple aspects of daily life[150] and viewing one's collective activities in that realm will produce a detailed, intimate, individual portrait of the user.[151]

---

148. *Id.* at 50.

149. United States v. Arnold, 454 F. Supp. 2d 999, 1000-01 (C.D. Cal. 2006), *rev'd*, 533 F.3d 1003 (9th Cir. 2008).

150. *See supra* note 7.

151. *Cf.* "mosaic theory" in United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (holding that government's attachment of global-positioning-system to undercarriage of motor vehicle, and use of that device to monitor vehicle's movements, constituted a search in violation of Fourth Amendment) ("I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."); *see* Cole, *supra* note 145, at 683.

The third fundamental precept is that case-by-case assessments are undesirable. Weighing the traditional tension between individual privacy and effective law enforcement for each individual situation is an ineffective model for deciding whether, and to what extent, to search digital devices at the border. Such a model would be inconsistent with *Riley*'s prerogatives.

The *Riley* Court recognized that assigning law enforcement officers the task of determining which type of cell phone data was searchable incident to arrest, or in what situations specific types of data might be searchable, would provide "no practical limit at all when it comes to cell phone searches,"[152] "impose few meaningful constraints on officers,"[153] and "launch courts on a difficult line-drawing expedition."[154] The Supreme Court rejected the prospect of a case-by-case analysis of which digital files can be searched incident to arrest.[155] The Court also rejected the prospect of creating rules that would allow partial searches, limited for example to call logs, which could be conducted incident to arrest.[156] Instead, *Riley* categorically asserted that any search of a cell phone seized incident to arrest requires probable cause.[157] The same concerns about imposing meaningful constraints and launching courts on line-drawing expeditions should apply to digital devices generally.

Even if case-by-case assessments were desirable, the approach is irreconcilably hindered by the fact that the terms "routine," "nonroutine," "forensic," and "manual" remain undefined. Although the search in *Cotterman* was deemed forensic, the Ninth Circuit did not define what a "forensic" search is.[158] "The majority never defines 'forensic,' leaving border agents to wonder exactly what searches are off-limits."[159] Thus even *Cotterman*, a case that establishes a rule that forensic searches are nonroutine and require reasonable suspicion, leaves the same challenge that led *Riley* to hold that all cell phone searches require a warrant. The

152. Riley v. California, 134 S. Ct. 2473, 2492 (2014).

153. *Id.*

154. *Id.* at 2493.

155. *Id.* at 2491.

156. *Id.* at 2492; *see supra* notes 15–19.

157. *Riley*, 134 S. Ct. at 2495.

158. United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013), *petition for cert. filed*, Petition for Writ of Certiorari, *Cotterman*, 2014 WL 491626, at *8–9 (2014) (No. 13-186); *see* Miller, *supra* note 117, at 1959 ("The Court has yet to define what searches would be 'nonroutine,' or what level of process it would impose for such searches.")

159. *Cotterman*, 709 F.3d at 978 (Callahan, J., concurring in part and dissenting in part).

fundamental question remains: what exactly is the difference between a "routine" and "nonroutine" border search of a laptop?[160]

The Ninth Circuit in *Cotterman* assumes that manual searches do not rise to the level of being intrusive enough to be deemed nonroutine.[161] Indeed, a one-minute view of a call log at the primary inspection area might well be considered routine and nonintrusive. It is not an extended border search. It does not view archives of personal data. A limited glance might very well be the true equivalent of quickly rifling through a pocket address book in the predigital era. Such a search would not in itself objectively trigger the privacy concerns about the massive amounts and unique types of data that a cell phone carries, nor raise questions such as the significance of viewing data that is stored in the cloud rather than on the physical device.

On the other hand, manual searches may expose a great deal of personal information. As one district court observed, "a manual search can be just as invasive as a full forensic examination."[162]

> [T]he privacy interests involved in searches of modern cell phones are present both during manual and forensic searches. While a forensic examination is more intrusive, a manual search of a modern cell phone certainly exposes the same type of information discussed in *Riley*—messages, photos, contacts list, call logs, etc.—both in isolated form and in combination.[163]

Even if the terms "routine" and "nonroutine" or "manual" and "forensic" could be defined with any certainty, the actual searches will fall on a sliding scale because each digital search will differ from the next. Searches of even identical devices may vary by actual files searched, length of time searched, whether images were viewed, whether an incriminating application was merely glimpsed or actually opened, whether the traveler voluntarily relinquished a password-protected file, and so on. Determining the point at which any given search transitions from a nonroutine to a

160. *See supra* Part III (discussing lack of a definition of the terms "routine" and "nonroutine" in *Cotterman*).

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

162. United States v. Ramos, 190 F. Supp. 3d 992, 1003 (S.D. Cal. 2016).

163. *Id.* at 1001; *see* Orin Kerr, *What is the Ninth Circuit's Standard for Border Searches Under* United States v. Cotterman*?* VOLOKH CONSPIRACY (Mar. 11, 2013, 3:12 PM), http://volokh.com/2013/03/11/what-is-the-ninth-circuits-standard-for-border-searches-under-united-states-v-cotterman (raising some very good questions about the manual-forensic distinction of the *Cotterman* decision).

merely routine search or vice-versa poses the problematic case-by-case analysis that *Riley* already firmly proscribed in the cell phone context.

Accordingly, asking law enforcement to distinguish between a forensic, or "nonroutine" search, and a nonforensic, or "routine" laptop search would open up the same minefield of uncertainty that *Riley* rejected. To answer the question of what level of search is nonroutine, the courts would, once again, be forced to resort to a balancing test of weighing the level of intrusiveness, or physical destruction, against the strength of the government interest. This would create an endless spiral of case-by-case evaluations. In the *Cotterman* petition, the petitioner urged case-by-case assessments, arguing that the "justification" of "reasonable suspicion" was insufficient to validate the search because the Ninth Circuit should also scrutinize the search's "scope" and "manner."[164] The Supreme Court rejected the writ.[165]

B. An Alternative Paradigm

This Article reinforces the argument that the reasonable suspicion standard should be triggered for a search of any digital item at the border and proposes to take the elephant out of the room; to include outbound, as well as inbound travelers; and clarify the meaning of "criminal activity afoot."[166]

1. Take the Elephant Out of the Room

First, no distinction should be made between between routine and nonroutine, or forensic and manual, searches. The *Cotterman* petition reasonably argues that the holding created an overly broad, undefined, and

164. United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013), *petition for cert. filed*, Petition for Writ of Certiorari, *Cotterman*, 2014 WL 491626, at *4–6 (2014) (No. 13-186).

165. *Cotterman*, 709 F.3d 952, *cert. denied*, 134 S. Ct. 899 (2014).

166. *See* Terry v. Ohio, 392 U.S. 1, 30 (1968) ("We merely hold today that where a police officer observes unusual conduct which leads him reasonably to conclude in light of his experience that *criminal activity may be afoot* and that the persons with whom he is dealing may be armed and presently dangerous, where in the course of investigating this behavior he identifies himself as a policeman and makes reasonable inquiries, and where nothing in the initial stages of the encounter serves to dispel his reasonable fear for his own or others' safety, he is entitled for the protection of himself and others in the area to conduct a carefully limited search of the outer clothing of such persons in an attempt to discover weapons which might be used to assault him.") (emphasis added). This Article does not dissect the Circuit split created by *Cotterman*, which is documented by the dissent in *Cotterman* itself. *Cotterman*, 709 F.3d 9542, 983 (M. Smith, J., dissenting) ("[T]he court creates a circuit split regarding the application of reasonable suspicion to border searches of electronic devices"; citations to Third and Fourth Circuit cases omitted); *see* Abidor v. Napolitano, 990 F. Supp. 2d 260, 281 (E.D.N.Y. 2013).

unworkable rule.[167] The unworkability, however, arises from the Ninth Circuit's decision being contingent on distinguishing "routine" from "nonroutine" digital searches.

This Article proposes that the elephant be taken out of the room: the reasonable suspicion standard should be triggered for border digital device searches—not because they are considered nonroutine, but because they are digital devices. The *Riley* Court rejected distinguishing between different levels of a cell phone search.[168] In the same manner, courts should reject distinguishing between routine and nonroutine levels of intrusiveness for a digital device border search. The fact that a cell phone may be on the person incident to arrest did not insulate the cell phone from the requirement of a warrant. The search incident to arrest exception did not justify dispensing with a warrant requirement before officers could search digital data on cell phones under either the traditional concern for the officers' safety or fear of destruction of evidence.[169] Likewise, the fact that a digital device is on the traveler should not insulate the digital device from the requirement of reasonable suspicion. While the distinction between routine and nonroutine works for searches of containers and human bodies, the concepts are inapposite to digital data.[170]

The proposal that all digital searches, whether manual or forensic, be generally considered nonroutine is a step in the right direction.[171] The landscape can be clarified even further by establishing that all digital border searches should require reasonable suspicion, without even the contingency of categorizing digital border searches as nonroutine. *Riley* did not require a warrant for a cell phone search because the search would be intrusive; indeed, evidence of the crime of arrest may well be discovered in a cursory, as well as extensive, search of a cell phone. *Riley* simply

167. United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013), *petition for cert. filed*, Petition for Writ of Certiorari, *Cotterman*, 2014 WL 491626, at *8 (2014) (No. 13-186).

168. Riley v. California, 134 S. Ct. 2473, 2491–93 (2014).

169. *Id.* at 2485–88.

170. Just in September 2016, one court even took the position that the routine/nonroutine framework has relevance only in intrusive searches of the person; thus, without directly saying so, this decision suggests, like this Article, that digital searches should not be classified as either routine or nonroutine. In *Czarnecki v. United States*, the district court aligned itself with the Government's position "that both the United States Supreme Court and the Ninth Circuit have rejected the routine/nonroutine framework for analyzing border cases. The Ninth Circuit has stated that . . . the Supreme Court 'made clear that a showing of "reasonable suspicion" was not required simply because the search went beyond a "routine" search.'" Czarnecki v. United States, No. C15-0421JLR, 2016 WL 5395549, at *8 (W.D. Wash. Sept. 27, 2016) (citation omitted). Thus, the district court stated that it "is inclined to agree with the Government that '[a]t most, the routine/non-routine framework is limited to "intrusive searches of the person" such as the alimentary canal search in *Montoya de Hernandez*.'" *Id.* at *8 (citation omitted).

171. *See* Miller, *supra* note 115, at 1995–96.

required a warrant for any search of a cell phone seized incident to arrest.[172] Likewise, no need exists to categorize digital searches as nonroutine in order to trigger the reasonable suspicion requirement. This Article therefore suggests that the terms "routine" and "nonroutine" be removed from the vernacular for describing digital searches. In this way, finally, the elephant can be coaxed out of the room.

Requiring "reasonable suspicion" even for mere "manual" searches, assuming there is agreement as to what that even means, formalizes the *de facto* process. The reality is that agents have limited resources to search every electronic device that passes through the country's borders and are limited to searching those devices where the traveler's conduct rouses some type of suspicion anyway:

> The greatest obstacle to ferreting out contraband at the border has always been the sheer number of international travelers. Any contention that national security will be critically hampered by stripping border agents of a critical law enforcement tool—suspicionless forensic examinations of electronics—is undermined by the fact that, as a matter of commonsense and resources, it is only when reasonable suspicion is aroused that such searches typically take place. *See, e.g.*, *Chaudhry*, 424 F.3d at 1054 (B. Fletcher, J., concurring) ("As a practical matter, border agents are too busy to do extensive searches (removing gas tanks and door panels, boring holes in truck beds) unless they have suspicion."). As Judge Callahan acknowledges in her separate opinion, the record suggests that "remote and/or intensive searches of electronic devices crossing the border do not occur all that often." Concurrence at 978 n. 11. The reference that only a small fraction of travelers at the border have their devices searched simply reinforces our point—our ruling will not place an undue burden on border agents who already rely on a degree of suspicion in referring travelers to secondary inspection.[173]

172. *Riley*, 134 S. Ct. at 2495.

173. United States v. Cotterman, 709 F.3d 952, 967 n.14 (9th Cir. 2013); *see id.* at 978 n.11 (Callahan, J., concurring in part and dissenting in part) (perceiving that border agents are able to conduct few intensive searches of electronic devices, but concluding that requiring reasonable suspicion for such searches is therefore unnecessary). *See also* Nadkarni, supra note 119, at 192; United States v. Romm, 455 F.3d 990, 1006 (9th Cir. 2006).

"Reasonable suspicion" imposes the minimal requirement for suspicion that is more than the next level of process, which is no suspicion at all.[174] Yet, instituting reasonable suspicion as a requirement for all digital searches acknowledges travelers' expectation of privacy in digital devices at the border—without encumbering agents' ability to do their job. "This standard is far from onerous and still leaves officers with considerable freedom to search suspicious persons and respond to unexpected factual developments."[175]

Finally, the exigent circumstances exception left open in *Riley* can similarly apply at the border to allow agents to conduct a search without even reasonable suspicion, if exigent circumstances arise. It is hard to imagine what such a scenario might look like, but just as *Riley* left the door open for allowing a warrantless search of cell phone data when faced with "some of the more extreme hypotheticals that have been suggested,"[176] a court may likewise leave the door open for a digital search without any particularized suspicion whatsoever, if faced with an "extreme" scenario. "[C]ustoms officials retain the ability to conduct suspicionless searches of cell phones in situations falling under the exigent circumstances exception."[177]

"Routine" and "nonroutine" are awkward fulcrums for determining the intrusiveness of the digital search and whether reasonable suspicion consequently is required. *Riley* held simply, "Get a warrant." The corollary at the border should be, "Get reasonable suspicion"—not because the search is forensic or nonroutine, whatever those terms mean—but because it is a digital device.

174. *See id.* at 960 ("Our review necessarily encompasses a determination as to the applicable standard, no suspicion, reasonable suspicion or probable cause."); *see also* United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013), *petition for cert.* Petition for Writ of Certiorari, *Cotterman*, 2014 WL 491626, at *3 (2014) (No. 13-186); Abidor v. Napolitano, 990 F. Supp. 2d 260, 276 (E.D.N.Y. 2013).

175. United States v. Saboonchi, 990 F. Supp. 2d 536, 570 (D. Md. 2014) (citations omitted). Even in a case where the court determined that reasonable suspicion was not needed because the search of the laptop was nonforensic, whereas *Cotterman* requires reasonable suspicion only for forensic examinations, the agent's initial search was motivated by reasonable suspicion, i.e., a travel itinerary that suggested involvement in narcotics trafficking. Kennedy v. United States, No. C12-1088RAJ, 2014 WL 954872, at *1–2 (W.D. Wash. Mar. 11, 2014); *see* Jon Adams, *Rights at United States Borders*, 19 BYU J. PUB. L. 353, 365 (2005) (stating that reasonable suspicion can be found by "[a]n itinerary suggestive of wrongdoing, (*e.g.* traveling to or from a country known for exporting drugs)" (citations omitted)).

176. Riley v. California, 134 S. Ct. 2473, 2494 (2014).

177. United States v. Ramos, 190 F. Supp. 3d 992, 1003 (S.D. Cal. 2016).

2. *Clarify Border Search to Include Outbound Travelers; Clarify the Meaning of "Criminal Activity Afoot"*

While requiring reasonable suspicion for all digital device border searches recognizes individual privacy interests, law enforcement needs will also be recognized by clarifying border searches to include inbound and outbound travelers and the meaning of "criminal activity afoot."

a. Include Inbound and Outbound Travelers

Guidance is needed as to whether a "border search" includes exit from, as well as entry into, the United States. This Article proposes that, just as a digital device does not fit the traditional physical container model, searching a digital device should not be limited to physical entry into the country's boundaries.

The Customs and Border Patrol Directive states that border search guidelines apply to "both inbound and outbound" travelers carrying electronic devices.[178] However, numerous courts have questioned whether the border search doctrines apply to those leaving the United States.

In *United States v. Kim*, the court took exception to the fact that the defendant was exiting, rather than entering, the country. The court noted that "[w]hile there is authority that states that the government's broad authority at the border extends to those exiting the country as well as to those coming in . . . the justifications for the exception to the warrant requirement are generally framed in terms of threats posed at the point of entry."[179]

One year later, in *United States v. Kolsuz*, the district court observed similarly that while the government has "a significant interest at the border in protecting its territory and national security 'by stopping and examining persons crossing into this country,' . . . the Supreme Court has consistently justified the government's interests at the border 'in terms of threats posed at the point of entry.'"[180] Thus, "none of the significant government interests in monitoring what *enters* the country applies where, as here, the

178. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE BORDER SEARCHES OF ELECTRONIC DEVICES (2009). The Immigration and Customs Enforcement Directive 7-6.1 similarly mandates that its directive "applies to searches of electronic devices of all persons arriving in, departing from, or transiting through the United States . . . ."

179. United States v. Kim, 103 F. Supp. 3d 32, 56 (D.D.C. 2015) (citations omitted); *see* United States v. Seljan, 547 F.3d 993, 999 (9th Cir. 2008) ("Because searches at the international border of both inbound and outbound persons or property are conducted 'pursuant to the long-standing right of the sovereign to protect itself,' they generally require neither a warrant nor individualized suspicion."); *see also* United States v. Cardona, 769 F.2d 625, 629 (9th Cir. 1985) ("[T]here is no principled basis to conclude that the extended border search doctrine does not apply with equal force to exit searches as it does to entry searches.").

180. United States v. Kolsuz, 185 F. Supp. 3d 843, 857 (E.D. Va. 2016).

object of a warrantless border search was *exiting* the country."[181] From there, the court deduces, rather awkwardly, that "[t]his interest is not directly implicated where, as here, a government agent conducts a forensic search of a cell phone, as the digital contents of a cell phone are not banned by export control regulations."[182]

Even more recently, the district court in *United States v. Feiten* emphasized entry, versus exit, at the border: "[T]he Supreme Court has recognized a broad exception to the Fourth Amendment's requirement of probable cause or a warrant for searches conducted at the border because [t]he Government interest *in preventing the entry of unwanted persons and effects* is at its zenith at the international border."[183]

Digital devices pose threats that traditional "merchandise" and "baggage"[184] did not. Again, the attempt to force "eighteenth-century principles"[185] upon current realities of twenty-first century travel creates incongruity and loses sight of the policies behind the principles. The policy of the United States border exception seeks to "protect itself from terrorist activities, unlawful migration, and contraband."[186] In the digital era, national security is no less threatened by the electronic devices of an outbound, than of an inbound, traveler. The spatial-temporal irrelevance of digital technology[187] makes concerns about ingress versus egress inapposite. The government indeed has an interest in preventing crimes that can be committed by taking data out of, as well as into, the country: not just child pornography, but also intellectual property thefts; commercial profit from data banned for export such as software and technology, or government secrets; and terrorist activity, to name a few examples. The CBP Directive needs the support of the courts.

b. Clarify the Meaning of "Criminal Activity Afoot"

Just as the distinction between entry and exit no longer makes sense in the temporal and spatial vacuum of digital devices, the argument that a border search must involve an ongoing or imminent crime makes little

181. *Id.* at 857–58.

182. *Id.* at 858.

183. United States v. Feiten, No. 15-20631, 2016 WL 894452, at *5 (E.D. Mich. Mar. 9, 2016) (internal citations and quotations marks omitted) (emphasis added).

184. U.S. DEP'T OF HOMELAND SEC., *supra* note 178 ("While the terms 'merchandise' and 'baggage' are used, the courts have interpreted border search authorities to extend to all of a traveler's belongings, including electronic devices and the information in such devices.").

185. United States v. Kim, 103 F. Supp. 3d 32, 51 (D.D.C. 2015).

186. KIM, *supra* note 41, at 1; *see* Cole, *supra* note 145, at 680 (citing Jennifer Daskal, *The Un-territoriality of Data*, 125 YALE L.J. 326, 329 (2015)).

187. *E.g., see generally* Rechtin, *supra* note 108.

sense in the digital era. First, a threat is not better poised to be committed simply because a digital device is entering, versus exiting, the United States; moreover, whether a crime is imminent or not may be unascertainable when the threat is housed in digital form. A threat from digital devices lies not in the physical hardware of the device entering a geographic territory, but in its data. That data may not even be stored in the hard drive of that specific device, but in fact in the cloud. A focus on ongoing or imminent crimes assumes that a threat takes a tangible form that can be intercepted at a certain point in time before damage can be done. This assumption is incongruous with threats created by the temporally and spatially irrelevant universe of digital devices.[188]

Second, a number of courts that have grappled with the issue of whether the border search of a digital device needs to involve an imminent crime have determined this to be a non issue, focusing instead on balancing the nature and intrusiveness of the search.[189] In *United States v. Ramos*, the court was unswayed by Defendant's attempts to argue that the search of his cell phone at the United States-Mexico border was not a border search, because the purpose was "investigatory."[190] Not only was there no authority "to suppor[t] the proposition that a border search is somehow converted into a search incident to arrest if its nature is 'investigatory,'" but "[a]dditionally, the word 'investigatory,' used as a qualifier by Defendant, is not helpful here. If the word "investigatory" in this context means further exploration into the possibility of a crime being committed, every border search would be investigatory in nature."[191]

188. *See generally id.*; *see also* Daskal, *supra* note 186, at 366 ("[D]ata differs from its tangible counterparts . . . ." Unlike data, "[p]hysical objects moving from place to place are constrained by the ordinary laws of physics and by generally observable and conscious choices about how to move from Point *A* to Point *B*.").

189. *See, e.g.*, United States v. Leininger, No. 16-CR-1530-GPC, 2016 WL 6476310, at *7 (S.D. Cal. Nov. 2, 2016); United States v. Hernandez, No. 15-CR-2613-GPC, 2016 WL 471943, at *2–3 (S.D. Cal. Feb. 8, 2016).

190. United States v. Ramos, 190 F. Supp. 3d 992, 999–1000 (S.D. Cal. 2016).

191. *Id.* at 999. The court distinguished *United States v. Kim*, 103 F. Supp. 3d 32 (D.D.C. 2015), where the court determined that "'[t]here was little or no reason to suspect that criminal activity was afoot at the time Kim was about to cross the border,'" because there "it was the combination of many factors . . . that led the court to determine that under the 'unique circumstances of this case,' the search was unreasonable. At no time did the court adopt the defendant's position that the investigatory nature of a search disqualifies it as a border search." *Id. See also Hernandez*, 2016 WL 471943 at *2 ("Hernandez argues that a distinction should be made between 'investigatory' border searches and 'protecting the United States sovereign integrity by excluding wanted persons or things.' . . . [However,] the distinction drawn by the Ninth Circuit was not whether the initial border search had an 'investigatory' function, but the nature and intrusiveness of the initial border search.").

Another court similarly concluded that a border search supported by reasonable suspicion will be upheld even when the relevant international travel was not clearly related to the suspicion of ongoing or imminent criminal activity.[192] In *United States v. Touset*, the district court held that Customs appropriately conducted a forensic search of Defendant's devices at the border based on the Department of Homeland Security Investigations' instructions that the Defendant's electronic media should be thoroughly inspected when he attempted to reenter the United States from abroad for possible possession of child pornography.[193] The court focused on the objectively reasonable search, which was substantiated by reasonable suspicion, and dismissed concerns about the purview of customs and agents' motivations. "As one Magistrate Judge has concluded, '[t]here is . . . little doubt that preventing the flow of contraband across the United States' borders, which would include illicit images of child pornography, falls within the purview of customs enforcement.'"[194] Thus, "'[t]hat interdiction of contraband can serve both customs and law enforcement purposes does not negate the validity of a search at the border.'"[195] Indeed, held another court, "[o]fficial interagency collaboration, even (and perhaps especially) at the border, is to be commended, not condemned."[196]

192. United States v. Touset, No. 1:15-CR-45-MHC, 2016 WL 1048047, at *11 (N.D. Ga. Mar. 11, 2016) (citing United States v. Saboonchi, 990 F. Supp. 2d 536, 571 (D. Md. 2014)).

193. *Touset*, 2016 WL 1048047, at *3.

194. *Id.* at *11 (citations omitted); *see* United States v. Smasal, No. CRIM. 15–85 JRT/BRT, 2015 WL 4622246, at *9–10 (D. Minn. June 19, 2015).

195. *Touset*, 2016 WL 1048047, at *11 (citing United States v. Flores-Montano, 541 U.S. 149, 150 (2004)); *see Smasal*, 2015 WL 4622246, at *10. Moreover, the district court in *Touset* held that even if a distinction exists between detentions based on law enforcement, versus customs enforcement, the customs agent's motivation is not the court's concern, as long as the arrest is objectively justifiable. *Touset*, 2016 WL 1048047 at *11–12 (citations omitted). "[C]oncerns about improper motives and pretext do not justify subjective inquiries' in the Fourth Amendment Context, and . . . '[e]fficient and evenhanded application of the law demands that we look to whether the [defendant's] arrest is objectively justified, rather than to the motive of the arresting officer." *Id.* at *12 (quoting Ashcroft v. al-Kidd, 563 U.S. 731, 740 (2011) (internal quotation marks omitted).

196. United States v. Levy, 803 F.3d 120, 123 (2d Cir. 2015) ("Whether a Customs official's reasonable suspicion arises entirely from her own investigation or is prompted by another federal agency is irrelevant to the validity of a border search, which we have held 'does not depend on whether it is prompted by a criminal investigative motive.'") (citing United States v. Irving, 452 F.3d 110, 123 (2d Cir. 2006)); *see also* United States v. Cano, No. 16–cr–01770–BTM, 2016 WL 6920449, at *3–4 (S.D. Cal. Nov. 23, 2016) ("[B]order search cases do not turn on the purpose or motivation behind the search. Rather, they focus on the degree of intrusiveness in light of the sovereign's interest at the border . . . . The Ninth Circuit's holding in *Cotterman* did not depend on whether the search was 'investigatory' in nature . . . . In fact, several courts in this District have refused to decide cases involving searches at the border on such a distinction.").

Moreover, once a search of electronic devices is underway, any efforts to distinguish between a search for an ongoing crime versus a search that is investigatory in nature lose meaning. One court skirted Defendant's contention that "the search in this case was intended to enforce the criminal laws and not to protect the borders from contraband."[197] The district court first reiterated that "border searches form 'a narrow exception to the Fourth Amendment prohibition against warrantless searches without probable cause," and that "'[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border.'"[198] The court then simply concluded that the Cellebrite border search of Defendant's electronic devices, after a dog alerted to the dashboard of the vehicle, which led to the discovery of ten packages of cocaine, was a "non-forensic scan . . . [that] accessed information available to any manual user examining electronic devices."[199] Moreover,

> The fact that the iPhone and the iPad were password protected using the Defendant's date of birth did not transform the Cellebrite search into the type of computer forensic examination used in *Cotterman*. Even assuming, however, that the password protection on the iPhone and iPad required additional constitutional protections, any requirement for reasonable suspicion would have been met in this case. The agents were investigating the smuggling of controlled substances into the United States.[200]

Thus, without actually saying so, the court dismissed Defendant's contention that any distinction should be drawn between enforcing criminal laws versus protecting the borders from contraband, and rejected the assertion that the border search was overbroad and lacked reasonable suspicion.

In line with these cases, this Article urges that, just as efforts to require reasonable suspicion for digital device searches by distinguishing between routine and nonroutine searches creates an unmanageable quagmire, efforts to limit digital device searches by distinguishing between investigatory and imminent crime searches creates a similarly

197. United States v. Lopez, No. 13CR2092 WQH, 2016 WL 7370030, at *2 (S.D. Cal. Dec. 20, 2016).

198. *Id.* at *3 (citing United States v. Seljan, 547 F.3d 993, 999 (9th Cir. 2008) and *Flores-Montano*, 541 U.S. at 149).

199. *Id.* at *4.

200. *Id.*

unmanageable quagmire. Finding reasonable suspicion should be the hurdle, not distinguishing between ongoing and imminent activity.

In sum, defining "criminal activity afoot" at the border without being bound to a perception of crime as unfolding in a linear manner is consistent with those courts that have already recognized the contradictions in excluding searches that might be deemed merely investigatory. Paired with including both inbound and outbound travelers, eliminating this distinction, in harmony with a bright-line rule requiring reasonable suspicion for all digital device searches, would help provide the balance that is now needed between individual privacy expectations in the rapidly evolving world of personal electronic devices and law enforcement interests in searching them.

Conclusion

It is only a matter of time before the digital search at-the-border issue is ripe and addressed before the United States Supreme Court. A rule is necessary that will protect national security interests while accommodating the new reality that ordinary, non-nefarious travelers, "[a]s denizens of a digital world . . . [will] carry with them laptop computers, iPhones, iPads, iPods, Kindles, Nooks, Surfaces, tablets, Blackberries, cell phones, digital cameras, and more,"[201] all of which are capable of carrying personal information in volumes unanticipated when the Supreme Court imagined drivers of vehicles carrying "containers."[202] Since the 2014 *Cotterman* decision, we may add Apple watches and Google glasses to the list, and this list will only continue to grow. The CBP Directive defines the category more simply: "Electronic Device. Includes any devices that many contain information . . . ."[203]

Some courts have already begun to propose reasonable suspicion, or even something more, as the threshold for digital searches at the border.

In April 2016, the district court in *United States v. Caballero* observed that the issue of whether a "cursory search of Defendant's cell phone" at the border search violates the Fourth Amendment "stands at the intersection of two avenues of law."[204]

> Heading in one direction is the Supreme Court's bright line rule in *Riley*: law enforcement officers must obtain a

201. United States v. Cotterman, 709 F.3d 952, 956 (9th Cir. 2013).

202. New York v. Belton, 453 U.S. 454 (1981).

203. *See* U.S. DEP'T OF HOMELAND SEC., *supra* note 178.

204. United States v. Caballero, 178 F. Supp. 3d 1008, 1014 (S.D. Cal. 2016).

> warrant to search a cell phone incident to an arrest. Heading on a different course is the border search exception . . . [that] describes an exception to general Fourth Amendment principles. It is the notion that the government may search without a warrant anyone and anything coming across its border to protect its national sovereignty. . . . But, neither the Supreme Court, nor the Ninth Circuit, has decided a case involving the heightened privacy interests implicated by a cell phone search at the border after an arrest.[205]

The court, bound by *Cotterman*, concluded that the warrantless, cursory search of defendant's cell phone was permissible under the border search doctrine with a showing of something less than reasonable suspicion, while an extensive search would have required reasonable suspicion.[206] However, "[i]f this [c]ourt were free to decide the question in the first instance, it would hold that the warrantless cell phone search under these circumstances would be unreasonable."[207] While the court expressed some reservations about applying the *Riley* standard of probable cause at the border,[208] the court emphasized its greater concern that "a cell phone search threatens significant individual privacy interests," and reiterated the concern expressed by the Supreme Court in *Riley* that "cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[209] Thus, "[a]lthough *Riley* could be applied to a cell phone search at the border, this [c]ourt is bound by *Cotterman*."[210]

Similarly, in June 2016, the district court in *United States v. Ramos* stated that "[a]dopting the reasonable suspicion standard currently used only for forensic examinations of digital devices . . . as the standard for all border searches of cell phones[] may be a prudent way to harmonize *Riley's* concerns with the salutary border search principles."[211] In a footnote, the court observed, "Such a standard would also allay the concern expressed in *Riley* that ad hoc, case-by-case determination provides

205. *Id.* (internal citations omitted).

206. *Id.* at 1016.

207. *Id.* at 1017.

208. *Id.* 1017 n.9.

209. *Id.* at 1017–18 (quoting United States v. Camou, 773 F.3d 932, 943 (9th Cir. 2014) (quoting Riley v. California, 134 S. Ct. 2473, 2488–89 (2014)).

210. *Caballero*, 178 F. Supp. 3d at 1018.

211. United States v. Ramos, 190 F. Supp. 3d 992, 1003 (S.D. Cal. 2016).

insufficient direction to law enforcement."[212] Indeed, this Article urges that such a standard provides the balance that is needed between the critical interests of both law enforcement and the private individual.

The *Cotterman* and *Riley* decisions provide guidance needed for honoring the Fourth Amendment in the digital era. One district court recently "acknowledge[d] that '[i]t may be that the 'technology is different' rationale that led the *Riley* Court to treat an arrestee's cell phone differently from his wallet [in the country's interior] will one day lead the [Supreme] Court to treat' an individual's cell phone differently from other property at the border as well."[213] Indeed, along with other cases testing the government's limits on searches via drones, GPS trackers, cell phones, and genetic profiling, this issue of digital devices searches at the border is certain to re-emerge before the U.S. Supreme Court, with privacy implications for us all, at a time when we face threats from terrorists and xenophobes alike.

212. *Id.* at 1003 n.9.

213. United States v. Molina-Isidoro, No. EP-16-CR-1402-PRM, 2016 WL 8138926, at *8 (W.D. Tex. Oct. 7, 2016) (holding that search of defendant's cell phone at the border was supported by reasonable suspicion) (citing United States v. Guerrero, 768 F.3d 351, 360 (5th Cir. 2014).