BORDER SEARCHES IN A DIGITAL AGE: FINDING ALIGNMENT AMIDST A DILUTED RIGHT

Anne L. Kelley[*]

Abstract

Searches of electronic devices at the border present a *sui generis* situation that distinguishes them from traditional border searches of other physical property, such as a backpack, car, or piece of luggage. The traditional border search doctrine framework has challenged federal courts with regard to how to categorize searches of electronic devices at the border. Traditionally, border searches are divided into one of two categories: "routine" or "non-routine." Searches of electronic devices, however, do not fit neatly into either category. This is because they present privacy concerns that surpass those falling within the ambit of routine searches of property at the border. As a result, federal circuit courts are split as to what, if any, level of suspicion should be required for searches of electronic devices at the border. A common thread amongst these decisions, however, exsts in the circuit courts' application of the U.S. Supreme Court's analytical framework in *Riley v. California*. Though *Riley* did not involve a border search, it did involve the warrantless, forensic search of an individual's cell phone. Notably, federal circuit courts have reached different conclusions in their shared application of the *Riley* Court's reasoning to answer the question of what, if any, standard of suspicion should be applied to forensic searches of electronic devices at the border. Given the uniquely intimate nature of the information—as well as the breadth of storage capacity—contained in electronic devices, it seems unwise to presume that the balance of competing interests at the border (between individual privacy and national security) should be preemptively tipped in favor of the government as it currently is. This Note seeks to demonstrate why such a presumption is concerning, and advocates for a solution that realigns the compelling privacy interests that individuals have in their electronic devices with the Fourth Amendment protections traditionally afforded to them at the border.

---

* J.D., University of Florida Levin College of Law; B.A., Wake Forest University. I dedicate this Note to my parents, Rob and Jan Kelley, for giving me the confidence to pursue my goals. I would also like to thank Professor Kenneth Nunn, for providing me with an inspiring introduction into Criminal Law, and who graciously agreed to sponsor this Note. Finally, I would like to thank all of the editors on the *Florida Law Review*, without whom this Note would not have been possible.

INTRODUCTION

The warrantless, forensic searches of U.S. citizens' electronic devices[1] that commonly occur at the U.S. border raise important privacy concerns that do not exist in the warrantless searches of other items of personal property, such as a car or a piece of luggage. Because of their unique storage capabilities, and prevalent use in modern society to store highly sensitive and intimate information, searches of electronic devices, especially forensic searches—those in which the search is conducted offsite and which employ computer forensics to uncover data[2]—have been held as intruding upon the personal lives of travelers substantially more than searches of traditional items, such as a backpack, suitcase, or even car.[3] Indeed, technology's "dual and conflicting capability to decrease privacy and augment the expectation of privacy"[4] calls into question longstanding border search practices and principles for failing to account for differences in technological property.

At the border, the government is uniquely tasked with simultaneously honoring both a citizen's personal expectation of privacy and a citizen's broader expectation of national security, expectations that are inherhently at odds.[5] The ambiguous and somewhat turbulent history of Fourth Amendment jurisprudence—the unfortunate backdrop against which this tension lies—has only aggravated this issue. Still, the government must find a way to honor both: "The goals of liberty and safety may be in tension, but they can coexist—indeed the Constitution mandates it."[6]

---

1. CBP Directive 3340-049A, Border Searches of Electronic Media (2018) defines "Electronic Device" as "[a]ny device that may contain information in an electronic or digital form such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players." For purposes of this Article, electronic device is used primarily to refer to computers, tablets, disks, drives, and mobile phones. U.S. CUSTOMS & BORDER PROT., CBP DIRECTIVE NO. 3340-049A, BORDER SEARCHES OF ELECTRONIC MEDIA 2 (2018) [hereinafter CBP DIRECTIVE NO. 3340-049A].

2. U.S. CUSTOMS & BORDER PROTECTION, CBP PUBLICATION 0204-0709, INSPECTION OF ELECTRONIC DEVICES (2018) [hereinafter CBP PUBLICATION 0204-0709].

3. "Cell phones differ in both a quantitative and qualitative sense from other objects that might be kept on an arrestee's person." *See* Riley v. California, 573 U.S. 373, 393 (2014).

4. United States v. Cotterman, 709 F.3d 952, 965 (9th Cir. 2013), *cert. denied*, 571 U.S. 1156 (2014).

5. In determining whether a law enforcement practice is constitutional, courts must balance its promotion of legitimate government interests against the intrusion on an individual's Fourth Amendment rights. United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985); *see also Cotterman*, 709 F.3d at 966 (reaffirming that people have an expectation of privacy as well as an expectation of national security).

6. Floyd v. City of New York, 959 F. Supp. 2d 540, 556 (S.D.N.Y. 2013).

Specifically with regard to electronic devices, the issue of competing interests continues to challenge courts.[7] The complexity of the issue lies primarily in the fact that, despite the significant level of intrusion that searches of electric devices impose, courts and the U.S. Customs and Border Protection (CBP) alike continue to miscategorize such, conducting them in the same manner as traditional traveler items.[8] This practice is problematic, however, for it ignores the reality that the heightened privacy interest one has in his cell phone is simply incomparable to the otherwise minimal interest one has in traditional traveler items. As the late Supreme Court Justice Antonin Scalia wisely observed, "It would be foolish to contend that the degree of privacy secured by citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[9] And in reviewing the country's longstanding border search doctrine, rejecting this contention in regard to searches of electronic devices seems particularly foolish.

This Note addresses whether technology has disrupted traditional Fourth Amendment doctrines in such a way that they have now become outdated—particularly in regard to the border search exception as applied searches of electronic devices. To begin, Part I describes a brief history of the border search exception, its legal and constitutional bases, and the Supreme Court's well-established principles in applying the doctrine. Next, Part II lays out the present interpretations of how the traditional doctrine should apply against the modern backdrop of technology. Part III then ponders the effect of these diverging interpretations, addressing why their resolution matters to society. Part IV discusses the current split amongst U.S. Circuit Courts of Appeals, and the Supreme Court's refusal so far to intervene. Part V assesses the strengths and weaknesses of the two competing approaches that have emerged from the case law. Finally, Part VI concludes with recommended solutions.

I. HISTORY AND DESCRIPTION OF THE BORDER SEARCH DOCTRINE

Generally, the Fourth Amendment requires a warrant based on probable cause for law enforcement searches to be legal.[10] This principle is homogenous across the U.S. judicial system, finding its constitutional roots in "[t]he right of the people to be secure in their persons, houses,

7. Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 505 (2007) ("Among scholars, this state of affairs [of Fourth Amendment jurisprudence] is widely considered an embarrassment. The Court's handiwork has been condemned as 'distressingly unmanageable,' 'unstable,' and 'a series of inconsistent and bizarre results that [the Court] has left entirely undefended.'") (internal footnotes omitted).

8. CBP PUBLICATION 0204-0709, *supra* note 2.

9. Kyllo v. United States, 533 U.S. 27, 33 (2001).

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

papers, and effects."[11] There are, however, exceptions to this general rule.[12] One such exception covers the nation's borders.[13] Historically, all searches designated as "border searches" have automatically been exempt from the probable cause and warrant requirements.[14] A search is categorized as such when the location of the search occurs at a port of entry or international border.[15] Under the border search exception doctrine, the Supreme Court has made clear that "routine" border searches are per se reasonable and thus can be conducted without a warrant or even without any reasonable suspicion that criminal activity is afoot.[16] The Court reasons that routine searches at the border "from before the adoption of the Fourth Amendment, have been considered to be 'reasonable' by the single fact that the person or item in question had entered in our country from the outside."[17] The rationales underlying the border search exception extend to both exit and entry searches.[18]

In addition to deeming these "routine" searches inherently reasonable, the Court has also identified three situations in which searches at the border might not be per se reasonable, i.e., at least some particularized reasonable suspicion would be required before conducting the border search.[19] These "non-routine" searches include: (1) highly intrusive searches of the person; (2) destructive searches of property; and (3) searches conducted in a particularly offensive manner.[20] Three landmark decisions by the Supreme Court provide a helpful framework for understanding when a border search will be considered "non-routine," and thus requiring some level of suspicion before the government search can be conducted.

---

11. U.S. CONST. amend. IV.

12. Among the many exceptions to the warrant requirement, some of the most commonly discussed are: searches incident to arrest, stop and frisk *Terry* searches, searches with consent, inventory searches, searches in schools, automobile searches, the plain view doctrine, the open fields doctrine, the hot pursuit doctrine, the emergency aid doctrine, and exigent circumstances.

13. United States v. Ramsey, 431 U.S. 606, 619–20 (1977).

14. *Border Searches and the Fourth Amendment*, 77 YALE L. J. 1007, 1008 (1968).

15. The "functional equivalent" doctrine effectively extends the border search doctrine to all ports of entry, including airports within the United States. *See* Almeida-Sanchez v. United States, 413 U.S. 266, 272–73 (1973).

16. *Ramsey*, 431 U.S. at 619.

17. *Id.*

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

19. United States v. Cotterman, 709 F.3d 952, 973 (9th Cir. 2013) (Callahan, J., concurring).

20. *Id.*

A. United States v. Montoya de Hernandez

In *United States v. Montoya de Hernandez*,[21] the Court (expectedly) categorized a search of one's alimentary canal as "beyond the scope of a routine customs search" due to the intrusiveness of the search.[22] There, the Court dealt with the admissibility of cocaine found in the defendant's alimentary canal and discussed whether the search, which took place at the border, violated the Fourth Amendment.[23] The Court reiterated its longstanding principle that the Fourth Amendment's balance of reasonableness is qualitatively different at the international border, and that "Congress has granted Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order . . . to prevent the introduction of contraband into this country."[24] In its analysis, the Court stated that though individuals are protected against unreasonable searches and seizures at the border, the balance it must achieve—between pursuing a legitimate government interest in securing our borders versus protecting individual privacy—is "struck much more favorably to the Government at the border."[25]

However, the Court proved in *Montoya de Hernandez* that this tipping of the scale is not limitless. There are times when the government is not given deference, and instead must qualify a search—even one at the border—with reasonable suspicion. The Court specifically stated that the detention of a traveler at the border and subsequent search of that traveler beyond the scope of a routine customs search is justified at its inception if customs agents, "considering all the facts surrounding the traveler and her trip, reasonably suspect that the traveler is smuggling contraband in her alimentary canal."[26] Notably, in a footnote attached to its holding, the Court explicitly stated that it did not address what view it has on what level of suspicion, if any, is required for other border searches such as strip, body cavity, or involuntary x-rays.[27] Thus, on one end of the spectrum, the *Montoya de Hernandez* Court clarified the appropriate level of suspicion for the particular factual circumstance of individuals detained at the border and found possessing drugs in their alimentary canal, establishing it as a non-routine search requiring reasonable suspicion. Yet, at the other end of the spectrum, the Court left the prospect of additional instances of "non-routine" searches wide open by failing to

21. 473 U.S. 531 (1985).
22. *Id.* at 541; *see also Cotterman*, 709 F.3d at 975 n.6.
23. *Montoya de Hernandez*, 473 U.S. at 533.
24. *Id.* at 537.
25. *Id.* at 540.
26. *Id.* at 541.
27. *Id.* at 541 n.4.

dictate the level of suspicion to be universally applied in those cases. In sum, though direction was given, *Montoya de Hernandez* did not establish a bright-line rule.

B. United States v. Flores-Montano

Almost a decade later, the Court faced a slightly difference scenario, where customs officials recovered drugs from the gas tank of a vehicle at an international border port of entry. In *United States v. Flores-Montano*,[28] the Court ruled that the Government's interference with a motorist's possessory interest in his gas tank was justified by the Government's paramount interest in protecting the nation's border.[29] More generally, the Court held that "the Government's authority to conduct suspicionless inspections at the border includes the authority to remove, disassemble, and reassemble a vehicle's fuel tank."[30] The Court reasoned that the Government's interest in protecting the border is paramount in this particular factual instance because "smugglers frequently attempt to penetrate our borders with contraband secreted in their automobiles' fuel tank."[31] The Court stated that this security interest outweighs any individual privacy interest in a fuel tank, which is used for the sole purpose of holding fuel.[32] The dismantling and reassembly of a gas tank caused no harm and was not destructive of the car, the Court reasoned, leading it to characterize the search as nothing more than an inconvenience to the traveler and consequently not requiring the protections of a non-routine search.[33]

After *Montoya de Hernandez* and *Flores-Montana*, the definitional guidance on what constituted a routine search versus what constituted a non-routine search landed on a limited spectrum—a spectrum within which the question of how to analyze more technologically advanced pieces of property remained unanswered.

C. Riley v. California

The Court thankfully began to bridge this gap of technological confusion in the pathmarking case *Riley v. California*.[34] There, the Court answered the increasingly significant question of whether the police may, without a warrant, search digital information on a cell phone seized from

28. 541 U.S. 149 (2004).
29. *Id.* at 155–56.
30. *Id.* at 155.
31. *Id.* at 153.
32. *Id.* at 154.
33. *See id.* at 155.
34. 573 U.S. 373 (2014).

an individual who has been arrested (also known as the "search-incident-to-arrest" exception to the warrant requirement).[35] Until *Riley*, the Court had not yet addressed that question directly, and thus *Riley*—though not directly on point to issues involving border searches—has served as foundational in lower courts' analysis of searches of electronic devices at the border.

In *Riley*, the Court addressed two factual circumstances brought by separate cases—both of which required a decision as to how the search-incident-to-arrest exception applies to modern searches of cell phones.[36] Acknowledging the absence of more precise guidance from the founding era, Chief Justice John Roberts asserted that the determination is generally accomplished "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed or the promotion of legitimate governmental interests."[37] Ultimately, the *Riley* Court narrowly held that a warrant was required to search a cell phone seized incident to an arrest, but it clarified that "[o]ur holding . . . is not that the information on a cell phone is immune from search . . . ."[38] Importantly, the Court left open the possibility that there may be instances where a warrant is *not* required to search a cell phone.[39] Significant precedents were set nonetheless in *Riley*, as the Court ruled that in the specific context of searches of cell phones incident to an arrest, individual privacy concerns ultimately outweigh the government's need to search the phone without a warrant.[40]

Although the existence of the border search exception has been recognized in Fourth Amendment jurisprudence for decades, its scope is much debated—much like the search-incident-to-arrest exception in *Riley*. Though the cases previously discussed provide somewhat of a blueprint for courts in applying the border search doctrine to electronic devices, much ambiguity and contradiction have been left in their wake.

II. DIFFERENT INTERPRETATIONS OF THE APPLICABLE STANDARD AS APPLIED TO BORDER SEARCHES OF ELECTRONIC DEVICES

The historical arguments for how the border exception doctrine should apply to electronic devices produce different interpretations, just as the

35. *Id.* at 385.

36. *Id.* at 378.

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

38. *Id.* at 401.

39. "Moreover, even though the search incident to arrest exception does not apply to cell phones, other case-specific exceptions may still justify a warrantless search of a particular phone." *Id.* at 401–02.

40. *Id.* at 401.

present case law does. One historical view highlights the fact that the same Congress that proposed the Fourth Amendment in the Bill of Rights also enacted the first customs statute in 1789, which authorized customs officials to stop and examine any vehicle, person, or piece of baggage arriving in the United States on a suspicion that any merchandise subject to duty is being concealed; otherwise, it cannot legally be imported into the United States.[41] Supporters of this view claim that "[t]he historical importance of the enactment of this customs statute by the same Congress which proposed the Fourth Amendment is, we think, manifest[]" in demonstrating the validity of the present border search exception to the warrant requirement.[42]

The alternative historical view, however, argues that this fact alone is not dispositive.[43] Rather, it proposes that those same legislators may have passed the 1789 statute without considering fully the position to which they were about to commit the community.[44] A community's standards of reasonableness may have changed over time: future changes in facts or circumstances may indeed make unreasonable a search that would have been reasonable by the same standards in 1789.[45]

Take, for example, present day technology. Courts are unified in recognizing that the government's interest in protecting the nation is at its peak at the border.[46] They vary, however, in their interpretations of the degree of privacy interests a traveler has, and how those interests should be weighed against those of the government at the border.[47] With regard to electronic devices, the various interpretations of the border search exception as it relates to the privacy interests of individuals are particularly divided.[48]

III. WHY DOES DETERMINING A NEW STANDARD FOR ELECTRONIC DEVICES MATTER?

In the Fourth Amendment realm, technology has muddied legal waters that were once clear. Before the age of cell phones and laptops, searches of personal property at the border had minimal impact on a person's privacy beyond the search itself. Definitively resolving a reasonableness requirement was of little concern to courts because the border itself

41. Act of July 31, 1789, ch. 5, § 23, 1 Stat. 29, 43.
42. *See* United States v. Ramsey, 431 U.S. 580, 616–17 (1977).
43. *Border Searches and the Fourth Amendment*, *supra* note 14, at 1011.
44. *Id.*
45. *Id.*
46. *See infra* Part IV.
47. *See id.*
48. *See id.*

rendered the search per se reasonable. This viewpoint was readily accepted because the nature of the property items being searched raised no pressing concern from citizens with regard to an expectation of privacy. For example, individuals can reasonably expect non-intrusive (non-routine) searches of their baggage and perhaps outer clothing at the border and thus are able to prepare for such searches by controlling what contents are, or are not, brought along.[49] If an individual wanted to keep something out of the hands of the government at the border—a personal diary, for example—that individual simply need not travel with it. This ability to physically separate tangible items of property keeps government infringement at a minimum. With electronic devices, however, such practicality does not exist, making the government's reach in searching these items essentially limitless.

A. *Determining a Standard Matters Because of the Unique Nature of Electronic Devices*

Individuals undoubtedly possess a higher expectation of privacy in cell phones and laptops than they do in other items of property due to the intimate nature and unmatched amount of information stored on these devices. While the latter items have limits on the scope of search, the former have none.[50] For example, the current Apple smartphone has a standard capacity of sixteen gigabytes (and is available up to sixty-four gigabytes).[51] To put this into perspective, sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos. And this incredible storage capacity in turn allows for the information on such devices to convey far more than previously possible.[52] Even the most basic cell phones that sell for far less than smartphones can hold photographs, picture messages, text messages, internet browsing history,

49. *Border Searches and the Fourth Amendment*, *supra* note 14, at 1013.

50. "One of the most notable distinguishing features of modern cellphones is their immense storage capacity. . . . But the possible intrusion on privacy is not physically limited in the same way [as pieces of mail, luggage, etc.] when it comes to cell phones." Riley v. California, 573 U.S. 373, 393–94 (2014); *see also* Orin S. Kerr, *Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403, 404–05 (2013) ("Much of the information stored in a person's cellular phone is deeply personal.").

51. *See* Kerr, *supra* note 50, at 404.

52. "The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone." *Riley*, 573 U.S. at 394–95.

calendars, phone books, and so on.[53] The possible breadth of a search of an electronic device makes it significantly intrusive. Moreover, the interrelatedness of the information stored on one's electronic device (and subject to search) makes it difficult, if not impossible, for individuals to prepare such an item for a search and protect privileged or confidential information.[54]

Adding to this difficulty is the element of personal attachment individuals have to their electronic devices. Not only do most Americans own cell phones, but according to a 2013 Mobile Consumer Habits study, nearly 75% of smartphone users report being within five feet of their phones most of the time.[55] The Supreme Court agrees: "[I]t is no exaggeration to say that many of the more than ninety percent 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."[56]

Thus, an unexpected, forensic search of the data contained on one's cell phone or laptop—which ranges from e-mails, finances, photos, contacts, passwords, or personal health information—can be morally compromising for an individual. Similar to an intrusive search of one's body, a forensic search of one's electronic device is suspect in that it, by its very nature, exposes an individual in an unwanted way, affronting their dignity. "The exposure of confidential and personal information has permanence. It cannot be undone."[57] This undignified exposure of an individual's private life that results from conducting a warrantless search of their electronic device is explicitly uncontested by the Court.[58] It is thus perplexing why some federal courts refuse to acknowledge otherwise; the mere context of the border should not justify such a major infringement on an individual's privacy right.

---

53. *Id*. at 394.

54. "The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information – an address, a note, a prescription, a bank statement, a video – that reveal much more in combination than any isolated record." *Id.*

55. *Americans Can't Put Down Their Smartphones, Even During Sex*, JUMIO (July 11, 2013), https://www.globenewswire.com/news-release/2013/07/11/1195636/0/en/Americans-Can-t-Put-Down-Their-Smartphones-Even-During-Sex.html [https://perma.cc/4NG8-VFB2].

56. *Riley*, 573 U.S. at 395.

57. United States v. Cotterman, 709 F.3d 952, 966 (9th Cir. 2013).

58. *See Riley*, 573 U.S. at 395; *see also* United States v. Jones, 565 U.S. 400, 415 (2012) (discussing the nature of information revealed by the GPS data of individuals while also recognizing that "[d]isclosed in [GPS] data . . . will be trips indisputably private in nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney . . . .").

Moreover, the government's ability to use seized and searched digital information in a way distinct from any identifying information gathered from tangible property further justifies a higher expectation of privacy in electronic devices. Unlike the physical contents of luggage or cars, the digital contents of electronic devices can be copied via "mirroring" capabilities during a forensic search.[59] Also unlike the contents of luggage or cars, these digital copies of the owner's data are not returned and can be easily transmitted to other government agencies. In light of recent whistleblower revelations over the alarmingly intrusive surveillance technology and practices of the National Security Agency (NSA), it is naive to assume the data recovered in these warrantless border searches is cleanly erased in every instance.[60] Justice Sonia Sotomayor, in *United States v. Jones*, [61] expressed a similar concern in her discussion of the government's potential abuse of information collected via the GPS monitoring of individuals.[62] Surely, then, how federal courts choose to interpret what standard applies in such searches matters greatly to the American people.

B. *Determining a Standard Matters Because of the Number of Individuals Affected*

Ownership of electronic devices is pervasive across the United States. Specifically, 96% of Americans own a cell phone of some kind, and 81% of Americans own a smartphone.[63] Additionally, 78% of American households own laptop computers.[64] This is a substantial increase from

59. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 540–41 (2005) (explaining "the creation of a perfect 'bitstream' copy or 'image' of the original storage device," which "duplicates every bit and byte on the target drive including all files"); *see also* Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. RICH. L. REV. 1091, 1118 (2009) ("There is no need to return the bitstream copy to the owner; the owner has the original data in his possession all along, and the government presumably could retain the copy for extended, even infinite, periods of time once the analysis is complete, perhaps perpetually.").

60. This is a reference to the domestic spying revelations by Edward Snowden and Bill Binney, who revealed to the public highly questionable domestic spying practices of the NSA and large data storage facilities where such information is kept and stored for indeterminate amounts of time. *See generally* David Welna, *Before Snowden: The Whistleblowers Who Tried To Lift The Veil*, NPR (July 22, 2014, 4:44 AM), https://www.npr.org/2014/07/22/333741495/before-snowden-the-whistleblowers-who-tried-to-lift-the-veil [https://perma.cc/PJV2-STL7].

61. 565 U.S. 400 (2012).

62. "The government can store such records and efficiently mine them for information years into the future." *Id.* at 415 (Sotomayor, J., concurring).

63. Pew Research Center, *Mobile Fact Sheet, Mobile Ownership Over Time* (2018), http://www.pewinternet.org/fact-sheet/mobile/[https://perma.cc/3K5T-EHHL].

64. CAMILLE RYAN & JAMIE M. LEWIS, U.S. CENSUS BUREAU, ACS-37, COMPUTER AND INTERNET USE IN THE UNITED STATES: 2015 2 (2017).

previous years. In 2014, for example, only about 55% of Americans owned a smartphone.[65] And in 2011, a mere 35% of Americans owned a smartphone.[66] It is therefore fair to predict with some certainty that within the next decade, almost every American adult will own a smartphone, a laptop, or both.

In FY 2017, CBP conducted 30,200 border searches, both inbound and outbound, of electronic devices.[67] This was a substantial increase from FY 2016, where only 19,051 devices were searched.[68] Moreover, the current 100-mile zone is an increase from the 50-mile zone that CBP previously operated under. At the time the regulations establishing the 100-mile border zone were adopted, there were fewer than 1,100 border patrol agents nationwide; today, there are over 21,000.[69] Thus, the frequency and scope of searches, as well as the manpower available to conduct searches at the border, all continue to increase at an alarmingly significant rate.

IV. A SPLIT IN THE CIRCUITS

The differing historical interpretations of the border exception doctrine, and the degree of privacy rights individuals should expect with electronic devices, glaringly reveal themselves upon a close examination of the holdings amongst the U.S. Circuit Courts of Appeals. The U.S. Courts of Appeals for the Fourth and Ninth Circuits both assert that the relevant inquiry for searches of electronic devices at the border is one of reasonableness, and that this determination must account for differences in property.[70] Those circuits classify the forensic examinations used to search electronic devices as non-routine border searches that must be justified by particularized suspicion before examination occurs.[71] By contrast, the U.S. Court of Appeals for the Eleventh Circuit has

65. Pew Research Center, *supra* note 63.

66. *Id.*

67. *CBP Releases Updated Border Search of Electronic Device and FY17 Statistics*, U.S. CUSTOMS & BORDER PROT. (Jan. 5, 2018), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and#:~:text=CBP%20Releases%20Updated%20Border%20Search%20of%20Electronic%20Device%20Directive%20and%20FY17%20Statistics,-Release%20Date%3A&text=Approximately%200.007%20percent%20of%20arriving,searched%20(more%20than%2029%2C200) [https://perma.cc/RQC4-VHAM].

68. *Id.*

69. *The Constitution and the 100 Mile Border Zone*, AMERICAN CIVIL LIBERTIES UNION (June 2018), https://www.aclu.org/other/constitution-100-mile-border-zone [https://perma.cc/3FPE-TZZT].

70. United States v. Cotterman, 709 F.3d 952, 966 (9th Cir. 2013); United States v. Kolsuz, 890 F.3d 133, 146 (4th Cir. 2018).

71. *Kolsuz*, 890 F.3d at 146.

consistently held in cases as recent as 2018 that border agents need no justification whatsoever to detain and forensically search electronic devices of any American citizen returning from abroad, classifying such searches as "routine."[72]

A common thread in these split circuit court decisions is their use of the analytical framework employed by the Supreme Court in *Riley*. Though *Riley* did not involve a border search, it did involve the warrantless forensic search of an individual's cell phone that revealed criminal activity and resulted in that individual's arrest.[73] In *Riley*, the Court, after balancing the public's heightened privacy interest in their cell phones against the government's interests, held that the police must obtain a warrant to search the cell phones of people who have been arrested.[74] Notably though, the circuit courts reach different conclusions in their shared application of the *Riley* Court's reasoning to answer the question of what, if any, standard of suspicion should be applied to forensic searches of electronic devices at the border?

A. *History of the Circuit Split*

Among three circuits, two different approaches are used to confront searches of citizens' electronic devices at the border. The Ninth Circuit, reasoning that the breadth and intimacy of electronic devices implicates substantial privacy interests with individuals, concluded that reasonable suspicion is required.[75] The Fourth Circuit agreed, reviving the historical distinction between routine and non-routine searches of property to qualify its holdings that electronic devices require reasonable suspicion.[76] The Eleventh Circuit, however, has been unpersuaded by the Fourth and Ninth Circuits' lines of reasoning. In the recently decided *United States v. Vergara*,[77] the Eleventh Circuit laid the foundation for dismissing a reasonable suspicion requirement at the border by stating that *Riley* was not factually analogous, but it failed to answer the question definitively.[78]

---

72. United States v. Touset, 890 F.3d 1227, 1232 (11th Cir. 2018); United States v. Vergara, 884 F.3d 1309, 1312 (11th Cir. 2018).

73. Riley v. California, 573 U.S. 373, 382 (2014).

74. *Id.* at 401; Karen Gullo, *EFF to New York Appeals Court: No Warrantless Searches of Devices at the Border*, ELEC. FRONTIER FOUND. (May 16, 2018), https://www.eff.org/deeplinks/2018/05/eff-new-york-appellate-court-no-warrantless-border-device-searches [https://perma.cc/QP4E-355B].

75. *Cotterman*, 709 F.3d at 968.

76. United States v. Kolsuz, 890 F.3d 133, 145–46 (4th Cir. 2018).

77. 884 F.3d 1309 (11th Cir. 2018).

78. *Id.* at 1312–13. Notably, it was an internally divided court. In a dissenting opinion, Judge Jill Pryor posited that although the Court has consistently held that routine border searches

Notably, the Supreme Court has routinely denied certiorari to cases involving border search issues,[79] and thus has yet to address the increasingly complex question of whether border agents need some level of suspicion to forensically search an electronic device. In response, circuit courts have either failed to address the issue themselves by finding that reasonable suspicion existed per se, or have answered definitively but then qualified their determination by holding that the result would be unchanged regardless because reasonable suspicion already existed from the unique set of facts.

B. *The Eleventh Circuit's Interpretation*

In *Vergara*, the Eleventh Circuit held that the warrant requirement that the *Riley* Court upheld in regard to the search of defendant's cell phone was *not* applicable to searches at the border.[80] The court stated that border searches "never require a warrant or probable cause. At most, border searches require reasonable suspicion."[81] Though the court addressed the privacy concerns involved in a search of a cell phone, it declined to address the question of whether reasonable suspicion is required in such a search at the border.[82] Because the defendant did not challenge the district's court finding that reasonable suspicion existed regardless of whether the court required a finding of it, the court stated it need not answer those questions.[83]

In *United States v. Touset*,[84] the Eleventh Circuit applied similar logic, holding that the Fourth Amendment does not require any suspicion for forensic searches of electronic devices at the border.[85] There, the court discredited the argument that electronic devices should receive special treatment, stating that "the same could be said for a recreational vehicle filled with personal effects or a tractor-trailer loaded with boxes of documents."[86] However, the court qualified its potentially controversial

(those involving cars, ships, luggage) do not require any level of suspicion, the government's authority at the border "is not without limits" as the majority in that case tried to imply. *Id.* at 1315.

79. Vergara v. United States, 139 S. Ct. 70 (2018) (denying certiorari in the case below, United States v. Vergara, 884 F.3d 1309 (11th Cir. 2018)); Cotterman v. United States, 571 U.S. 1156 (2014) (denying certiorari in the case below, United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013)).

80. *Vergara*, 884 F.3d at 1311.

81. *Id.*

82. *Id.*

83. *Id.* at 1313. Vergara challenged the issue of whether warrantless forensic searches of two cell phones at the border violated the Fourth Amendment on appeal. *Id.*

84. 890 F.3d 1227 (11th Cir. 2018).

85. *Id.* at 1231.

86. *Id.* at 1233.

holding by stating that, in the event that reasonable suspicion was required, it existed in that particular set of facts.[87] This sort of judicial loophole—deciding not to answer the reasonable suspicion question because it already existed in that particular case—has been used by other courts confronting similar sets of facts as well.[88]

C. *The Fourth and Ninth Circuits' Interpretation*

In *United States v. Johnson*,[89] the Ninth Circuit established that probable cause in searches demands factual specificity and must be judged according to an objective standard.[90] "Anything less would invite intrusions upon constitutionally guaranteed rights based on nothing more than inarticulate hunches, a result [the Supreme Court] has consistently refused to sanction."[91] In that case, the court was considering whether the police needed probable cause to search the house under the exigent circumstances exception to searches.[92] The court made clear that when the government relies on the exigent circumstances exception to the Fourth Amendment's warrant requirement, it still must satisfy two requirements: proof that the officer had probable cause to search the house; and proof that the exigent circumstances justified the warrantless intrusion.[93] Although the court in *Johnson* was considering a different Fourth Amendment exception, the Ninth Circuit has consistently imposed similar requirements in cases involving the border search exception, helping to provide a foundational uniformity in the application of the Fourth Amendment to various search exception doctrines. Paralleling *Johnson*, the decision in *United States v. Seljan*[94] reaffirmed that the Ninth Circuit rejects an "anything goes"[95] approach at the border.

In *United States v. Cotterman*,[96] agents seized Cotterman's two laptops and camera from his vehicle at the U.S.-Mexico border in response to an alert based in part on a TECS alert revealing defendant's prior conviction for child molestation. [97] Agents subsequently conducted a forensic examination of the devices and discovered large amounts of

87. *Id.* at 1231–32.
88. *See supra* Sections I.B., I.C.
89. 256 F.3d 895 (9th Cir. 2001).
90. *Id.* at 905.
91. *Id.*
92. *Id.*
93. *Id.*
94. 547 F.3d 993 (9th Cir. 2008).
95. *Id.* at 1000.
96. 709 F.3d 952 (9th Cir. 2013).
97. *Id.* at 957.

child pornography.[98] In assessing the reasonableness of a forensic computer search—a search that began as a cursory review of Cotterman driving through the border, but that transformed into a forensic examination uncovering incriminating evidence—the court first established that a reasonable suspicion standard was appropriate.[99] In assessing the totality of circumstances, the court next concluded that the examination of Cotterman's electronic devices *was* supported by reasonable suspicion, and that the scope and manner of the search were both reasonable under the Fourth Amendment.[100] The court highlighted the powerfully intrusive scope of a computer forensic examination to justify its conclusion.[101] For the *Cotterman* majority, the concern was less about where the search was conducted and more about "what one is looking for and how one goes about searching for it."[102]

Using similar logic, the Fourth Circuit in *United States v. Kolsuz*[103] concluded that a forensic examination of a defendant's cell phone must be considered a non-routine border search.[104] As such, the court acknowledged that the search required some measure of individualized suspicion—whether reasonable suspicion is enough or if there must be a warrant based on probable cause—but declined to rule as to what the standard should be.[105] The *Kolsuz* court conceded that Supreme Court precedent makes clear that at the border (or at any of its functional equivalents), government agents may conduct *routine* searches and seizures without a warrant and even without any individualized suspicion.[106] What the *Kolsuz* court grappled with, however, was whether the search of a cell phone appropriately fell under that category. While acknowledging the lack of guidance from the Supreme Court on what precisely constitutes a non-routine search, the Fourth Circuit followed the

98. *Id.* at 956.

99. "It is the comprehensive and intrusive nature of a forensic examination—not the location of the examination—that is the key factor triggering the requirement of reasonable suspicion here." *Id.* at 962.

100. Thus, defendant's motion to suppress the evidence of pornography uncovered in the forensic search was denied. *Id.* at 970.

101. The majority went on to establish that "legitimate concerns about child pornography do not justify unfettered crime-fighting searches or an unregulated assault on citizens' private information. Reasonable suspicion is a modest, workable standard that is already applied in the extended border search, *Terry* stop, and other contexts." *Id.* at 966.

102. *Id.* at 962.

103. 890 F.3d 133 (4th Cir. 2018).

104. *Id.* at 137.

105. *Id.*

106. *Id.*

precedent of *Cotterma*n: forensic searches of digital devices seized at the border may properly be categorized as non-routine.[107]

The *Kolsuz* court cited three major factors in its determination. First, the court stated that the scale of data that can be stored on digital devices "dwarfs the amount of personal information that can be carried over a boarder—and thus subjected to a routine border search—in a luggage or a car."[108] Second, the court explained that "[t]he uniquely sensitive nature of that information matters" because "[s]martphones and laptops 'contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails . . . .'"[109] Third, the court clarified that:

> [W]hile an international traveler can mitigate the intrusion occasioned by a routine luggage search by leaving behind her diaries, photographs, and other especially personal effects, the same is not true, at least practically speaking, when it comes to smartphones and digital devices. Portable electronic devices are ubiquitous—for many, the most reliable means of contract when abroad—and it is neither "realistic nor reasonable to expect the average traveler to leave his digital devices at home when traveling."[110]

V. EVALUATION OF EACH INTERPRETATION

The two competing interpretations that presently exist regarding the level of suspicion necessary for border searches of electronic devices both exhibit meaningful rationale. However, neither is without reproach.

A. *Interpretation One: No Reasonable Suspicion Is Necessary*

The border search exception has long been justified by the vital national interest in preventing illegal entry and smuggling, particularly of narcotics.[111] The most basic argument underlying this interpretation is that border searches are considered differentiable as a class, and the fact that an individual has recently crossed a border *does* actually increase the probability that illicit materials may be present; travelers are a suspect class for this reason.[112] And the case law evidences that smugglers frequently attempt to penetrate our borders with contraband and other

107. *Id.* at 144.
108. *Id.* at 145.
109. *Id.*
110. *Id.*
111. *Border Searches and the Fourth Amendment*, *supra* note 14, at 1011.
112. *Id.* at 1018.

illicit materials.[113] Thus, the suspicionless searches that occur at the border are certainly beneficial in that they frequently expose and capture some of the most despicable criminals, from child pornographers to terrorists. The influential *Riley* Court acknowledges these points explicitly: "Cell phones . . . can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost."[114]

But—does it have to? *Riley*, in ultimately holding for a warrant requirement before officers can search a cell phone incident to an arrest, did not seem to think so: "Our cases have historically recognized that the warrant requirement . . . [is not] merely an 'inconvenience to be somehow "weighed" against the claims of police efficiency.'"[115] The assertion that protecting an individual's dignity—at issue in the context of electronic devices—must come at the cost of law enforcement's ability to combat crime is misguided, and the Supreme Court seems to consistently agree. Procedural requirements in searches and seizures are thought by the Court to be "an important working part of our machinery of government."[116] The border may necessarily dilute the traditional Fourth Amendment protections for travelers, but it should not erode them completely.

This view also points to the fact that despite individuals' prevalent ownership and dependency on electronic devices, the number of devices actually searched is only a small percentage of the whole.[117] But this fact does not help to combat the data revealing the steady growth in the number of searches conducted at the border. As established earlier, the overarching problem at the border is not that a minimal number of citizens are, in current practices, actually being affected, but that the *potential* for any number of citizens to be affected is great amidst the current judicial landscape.

Justice Stephen Breyer, in defense of suspicionless border searches, has pointed out that CBP keeps track of the border searches its agents conduct, including the reasons for the searches.[118] Though he was referring to gas tank searches, Justice Breyer's argument that this administrative process should alleviate concerns of abusive searches is unpersuasive. Keeping statistics does not, by itself, avoid discriminatory policy. Moreover, even if individuals were able to know the reasons for

113. United States v. Flores-Montano, 541 U.S. 150, 152–53 (2004).

114. Riley v. California, 573 U.S. 373, 401 (2014).

115. *Id.*

116. *Id.* (quoting Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971)).

117. *See CBP Releases Updated Border Search of Electronic Device and FY17 Statistics*, *supra* note 67 ("In FY17. . . . Approximately 0.007 percent of arriving international travelers processed by CBP officers had their electronic devices searched.").

118. *Flores-Montano*, 541 U.S. at 156 (Breyer, J., concurring).

CBP searches, such administrative retention records do not give them the more important privacy details at stake[119]—*who* has seen their data and *what* have they seen.

B. *Interpretation Two: Some Level of Suspicion is Required*

This second interpretation takes into account more than logic and bare constitutional language. Instead, its rejection of such a formalist approach embraces the role that societal values, background, culture, and real world experience should play in complex legal decisions. This viewpoint garners support from the simple fact that cell phone and laptop technology was inconceivable not only to the Founders when they wrote the Amendment, but also to the decisions underpinning the current case law just a few decades ago. The Supreme Court acknowledged this reality in *Riley*, when it explicitly recognized the outdated jurisprudence in which current Fourth Amendment issues must rest, and the hardship this poses on the Court in attempting to fashion an appropriate legal analysis to modern day technology.[120] Lower courts and commentators agree.[121]

The data makes clear that people utilize modern technology in extremely dependent and uniquely intimate ways. It follows that people's expectation of privacy in their electronic devices is at an all-time high, falling just under the level of privacy they expect for their physical body. Both the Court and the people agree. In *Riley,* the Court likened a person's cell phone to "an important feature of human anatomy." [122] The Ninth Circuit further colored these assertions in *Cotterman* by persuasive analogy. It stated that the "painstaking analysis" that occurs in a forensic search, which in *Cotterman* consisted of recovering information on a laptop that had ostensibly been deleted by the owner, "is akin to reading a diary line by line looking for mention of criminal activity—plus looking

---

119. CBP Directive requires Officers performing the search to complete after-action reporting requirements via Form 6051D, available at https://www.customsesq.com/wp-content/uploads/2019/04/Notice-of-Detention-Form-6051D.pdf [https://perma.cc/2CG7-9BRH]. This Form is a standardized, one-pager used for the detention of any detained property and requires a minimum level of detail. *See also* Rachel Flipse, Comment, *An Unbalanced Standard: Search and Seizure of Electronic Data Under the Border Search Doctrine*, 12 U. PA. J. CONST. L. 851, 869 (2010).

120. "Both phones are based on technology nearly inconceivable just a few decades ago, when *Chimel* and *Robinson* were decided." *Riley*, 573 U.S. at 387.

121. Formalism has, surprisingly and pervadingly, a renewed appearance to judges and lawyers in our technological era, even though it retards the profession's ability to solve the novel legal problems that arise in such an era. Legal realists are bound to find technology more congenial than legal formalists do—especially since technology is gaining on the law." RICHARD A. POSNER, REFLECTIONS ON JUDGING 8 (2013); *see also* Kerr, *supra* note 50, at 404–05.

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

at everything the writer may have erased."[123] And, importantly, citizens agree. For instance, the media coins such border searches as "digital strip searches,"[124] and a number of legal news and resource outlets have published memos warning citizens of the border search trends, providing useful tips for getting around the intrusive searches.[125] The Supreme Court has recognized that "the degree of community resentment aroused by particular practices is clearly relevant to an assessment of the quality of the intrusion upon reasonable expectations of personal security."[126] Framed in this way, the Fourth and Ninth Circuits present a compelling justification for their assertion that electronic devices meet a threshold of intrusiveness that justifies categorizing them as beyond the scope of a routine search.

In evaluating both interpretations, it seems that to ignore the *sui generis* nature of electronic devices in our modern day border search doctrine is to disservice the purpose of the Fourth Amendment and the very people it seeks to protect. Lower courts dealing with electronic devices and the border search exception almost exclusively rely on *Riley* to instruct them. However, doing so is to those courts' detriment. While the Eleventh Circuit is correct in that *Riley* was a limited holding that does not directly apply to border searches, the Fourth and Ninth Circuits are also correct in using *Riley*'s characterization of cell phones to guide their analysis and form the conclusion that border searches of electronic devices, despite being pieces of property, do not appropriately fit within the traditional category of a routine search.

VI. RECOMMENDED SOLUTIONS

The budding circuit split is the most concrete example of why *Riley*—despite being one of the only Supreme Court cases to deal with the intersection of the Fourth Amendment and modern technology—is

123. United States v. Cotterman, 709 F.3d 952, 962–63 (9th Cir. 2013).

124. Olivia Solon, *US Border Agents are Doing 'Digital Strip Searches.' Here's How to Protect Yourself*, GUARDIAN (Mar. 31, 2017), https://www.theguardian.com/us-news/2017/mar/31/us-border-phone-computer-searches-how-to-protect [https://perma.cc/U85P-FJSS].

125. Kelly T. Currie et al., *No Reasonable Suspicion Required for Forensic Searches of Electronic Devices at the Border*, CM TRADE LAW (May 25, 2018), https://www.cmtradelaw.com/2018/05/no-reasonable-suspicion-required-for-forensic-searches-of-electronic-devices-at-the-border/ [https://perma.cc/2M4Q-64D2]; Sophia Cope, *Law Enforcement Uses Border Search Exception as Fourth Amendment Loophole*, ELEC. FRONTIER FOUND. (Dec. 8, 2016), https://www.eff.org/deeplinks/2016/12/law-enforcement-uses-border-search-exception-fourth-amendment-loophole [https://perma.cc/8W97-ZLD2]; Karen Gullo, *supra* note 74; *see The Constitution in the 100-Mile Border Zone*, *supra* note 69.

126. Floyd v. City of New York, 959 F. Supp. 2d 540, 556–57 (S.D.N.Y. 2013) (quoting Terry v. Ohio, 392 U.S. 1, 17 n.14 (1968)).

insufficiently broad to deal with searches of electronic devices at the border. A thorough and accurate application of the Fourth Amendment and its border search exception to electronic devices will instead require a comprehensive review of the history, evolution, and related case law.

In attempting to balance the competing interests of today's government with the Fourth Amendment's constitutional roots, this Note recommends a compromising approach that seeks to realign the border search exception with longstanding Fourth Amendment jurisprudence in light of modern technology and cultural trends. That approach includes a two-fold movement by the courts and administrative agencies. The Supreme Court should pierce the mysticism surrounding its viewpoint on this issue and affirmatively establish that, as being beyond the scope of a routine search, electronic devices require some level of suspicion before a search can occur at the border. In addition, administrative agencies such as CBP and U.S. Immigration and Customs Enforcement (ICE) should update their policies and procedures with clear and consistent terminology.

A. *Judicial Activism by the Court: A New Balance*

This Note recommends that the Court reject the traditional balancing test which always weighs reasonable suspicion in the government's favor at the border. Courts should not mechanically apply the outdated rules of a predigital era to the search of a modern day cell phone. Instead, this Note calls for an approach similar to that of the Court in *Kyllo v. United States*, which takes the plain language of the Fourth Amendment and adapts its reading to fit modern times.[127] In that way, this Note's approach is in accord with the Fourth and Ninth Circuits' reasoning in their application of *Riley* to border searches.

B. *Electronic Devices Categorized as Non-Routine*

Given the traction this issue has gained over the last decade, this Note recommends that the Supreme Court conclusively categorize digital searches at the border as non-routine, affirming that at least *some* level of suspicion is necessary for such searches. This categorization would be in accord with both the Court's preexisting border search jurisprudence, as well as its decisions requiring a warrant for cell phones in other special searches, such as cellphones seized in a search incident to an arrest and in searches of automobiles.

In light of the strengths and weaknesses of the competing standards discussed above, it is clear that courts—especially the Supreme Court—

127. Kyllo v. United States, 533 U.S. 26, 35 (2001).

have long held that the critical factor in determining whether a search is routine or non-routine is the degree of intrusiveness. While the Court has yet to address the category of digital devices at the border, it has provided guideline by analogy on both the topic of intrusiveness and how it views cell phones so as to allow lower courts to answer whether electronic devices meet such a level of intrusiveness. Particularly instructive are those cases, discussed in Part I, in which the Court has dealt with border searches of alimentary canals and gas tanks, as well as the search of a cell phone incident to arrest in *Riley.* This Note's recommendation that border searches be deemed as intrusive enough to constitute a non-routine characterization aligns with the *Riley* Court and the longstanding test of reasonableness.[128] Interpreting the Court's decision in *Riley* to mean otherwise simply because of the border context—as the Eleventh Circuit has attempted to do—is to misread the Court's precedent-setting dicta on special searches of modern technology: "With all [cell phones] contain and all they may reveal, they hold for many Americans 'the privacies of life[.]'"[129]

This Note's argument for a realignment of Fourth Amendment principles to match modern technology additionally boasts compliance with a textualist view, for it seeks to preserve, above all, the Founding Father's original intent. The original customs statute of 1789 exempting searches from probable cause requirements was passed by the First Congress, which also proposed the Bill of Rights.[130] Similarly, a driving force of both the Revolutionary War and subsequent drafting of the Fourth Amendment was, in the words of John Adams, to "take arms"[131] against the writs of assistance and general warrants of the colonial era that allowed British officers to "rummage through homes in an unrestrained search for evidence of criminal activity."[132] Allowing the warrantless searches of electronic devices at the border because they are

128. "Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is." Riley v. California, 573 U.S. 373, 396 (2014).

129. *Id.* at 403.

130. "It has often been argued that this fact demonstrates the validity of the present border search exemption." *See Border Searches and the Fourth Amendment*, *supra* note 14, at 1011. *See also* Boyd v. United States, 116 U.S. 616, 623 (1886) (stating that because the Act of July 31, 1789 was passed by the same congress which proposed for the adoption of the original amendments to the constitution, "it is clear that the members of that body did not regard searches and seizures of this kind as 'unreasonable'" and are thus exempted from the category of unreasonable searches and seizures).

131. "Every man of a crowded audience appeared to me to go away, as I did, ready to take arms against writs of assistance." Letter from John Adams to William Tudor (Mar. 29, 1817).

132. *Riley*, 573 U.S. at 403.

characterized as "routine" would undoubtedly be to allow for a similarly unrestrained search for evidence of criminal activity the founding generation sought to avoid. An observation from Judge Learned Hand articulates this point: "[It is] a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him."[133] Equally, if not more so than the unique intimacies of one's home, modern electronic devices possess a *sui generis* capability that qualifies them for a non-routine categorization, *even* at the border.

It is undisputed that the plain text of the Fourth Amendment does not include a provision for technology. But to limit a reading of the Fourth Amendment to exclude protecting something that indisputably—both by the Court[134] itself and citizens alike—rises to the same level of expected privacy as that in one's person or home, would serve no loyalty to the Founding Fathers; it would simply be stubborn.

C. *A Reasonable Suspicion Standard Is Appropriate*

Having established that electronic devices are more appropriately categorized at the border as non-routine searches, this Note attempts to articulate the level of suspicion that courts should uniformly adopt. The historical determination of whether to exempt a given type of search from the warrant requirement is generally accomplished "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[135] But this should not be the only determination. It is important to note another longstanding governing principle, that the Fourth Amendment "protects people—and not simply 'areas.'"[136] Arguably, the current practices are protecting "the place" (the border) at all costs to the person. Requiring at least some level of suspicion would pay homage to the principle established in *Katz v. United States*[137] by ensuring that searches of electronic devices at the border are more protective of "the people" rather than the "place" being searched.

Neither was the Fourth Amendment designed to protect law enforcement over the people. Proponents of warrantless searches of electronic devices at the border point to efficiency concerns. But such

133. United States v. Kirschenblatt, 16 F.2d 202, 203 (2d Cir. 1926).

134. "The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." *Riley*, 573 U.S. at 403.

135. *Id.* at 387.

136. Katz v. United States, 389 U.S. 347, 353 (1967).

137. 389 U.S. 347 (1967).

concerns are baseless. "Recent technological advances . . . [have] made the process of obtaining a warrant itself more efficient."[138] Police officers can email warrant requests to judges' iPads, and there have been situations in which judges have signed such warrants and emailed them back to officers in less than fifteen minutes.[139] Nor has the Court described the border as constituting such an exigent circumstance excepting a search from the warrant requirement. *Riley* alluded to case-specific exceptions where a warrantless search of a phone may be justified, citing the "exigencies of a situation" as an example.[140] But there are a few reasons why the border should not qualify as such an exigency.

First, U.S. citizens, as opposed to undocumented persons or foreign travelers, should not be considered a "fleeing" suspect because law enforcement can easily trace citizens via registered home addresses, travel information, drivers license, and any other record of the sort. Law enforcement has demonstrated the ease of relying on such records to track and detain suspect individuals time and again. Second, cell phones, unlike a piece of luggage, which officers could reasonably believe to contain some "immediately dangerous instrumentality, such as explosives," [141] are rarely used in ways that pose imminent injury. Though cell phones do have the ability to potentially act as a remote detonator for an explosive device, the government has other, less intrusive means by which to detect such a situation, and the mere risk of such a rarely occurring event should not justify warrantless searches on a regular basis.[142] If the government did hypothetically detect such terrorist activity—possibly through a discrete technique such as cell phone jamming of the localized area—it would then in theory have the reasonable suspicion required to perform a permissible search and seizure of said device. The border itself, at least

138. *Riley*, 573 U.S. at 401.

139. Missouri v. McNeely, 569 U.S. 141, 173 (2013) (Roberts, C.J., concurring).

140. *Riley*, 573 U.S. at 402 (quoting Kentucky v. King, 563 U.S. 452, 460 (2011)).

141. The Court in *Chadwick* noted that in such a situation, "it would be foolhardy to transport [the luggage] to the station without opening the luggage." United States v. Chadwick, 433 U.S. 1, 15 n.9 (1977).

142. Cellular jamming is a method used to combat and detect devices modified for the purpose of detonating an explosive. It works by flooding radio channels with "jibberish signals, essentially crowding out the particular signal a cellphone is looking for." David Axe, *Cellphone Bombs: The New American Terror*, DAILY BEAST (Sept. 20, 2016), https://www.thedailybeast.com/cellphone-bombs-the-new-american-terror [https://perma.cc/83R2-SQ5N]. Though the practice is indiscriminate and thus could be problematic if done widespread, "cellphone jamming in a small or fixed area can be useful. Many prisons jam incoming signals. The U.S. Secret Service reportedly possesses jammers that accompany presidential motorcades." *Id.*

for citizens, does *not* constitute an exigent circumstance without more, and precedent agrees.

While the expectation of privacy is justifiably less at the border than in the interior, it still exists. A reasonable suspicion standard is an appropriate middle ground in realigning the border search doctrine with the paramount level of privacy interests individuals have in the information stored on their electronic devices.

D. *Reform Within the Administrative Agencies Involved*

Finally, this Note recommends that, at a minimum, CBP should update its 2018 policy[143] relating to the searching digital devices. Although the current CBP guidance requires reasonable suspicion for "advanced searches"[144] of electronic devices at the border, the practical implications of this policy, coupled with the divided case law, are insufficiently clear. This is because of the exception within CBP's guidance policy that allows for suspicionless forensic searches in cases of "national security concern."[145] Because courts adamantly reinforce that the government's national security concerns are at their "zenith" at the border,[146] the broadness of this phrase may allow CBP's policy exception to be invoked in potentially any border search context, simply because the search is at the border. Although the Directive attempts to cabin the broadness of what constitutes "reasonable suspicion" or a "national security concern," the two examples it cites to do so are unhelpful.[147] Undoubtedly, these policy ambiguities will force courts to play a role in interpreting what qualifies as a "national security concern." Yet, in light of their already problematic ventures in balancing traditional

143. CBP DIRECTIVE NO. 3340-049A, *supra* note 1.

144. "An advanced search is any search in which an Officer connects equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents." *Id.* at 5.

145. Jadzia Pierce, *CBP Revises Rules for Border Searches of Electronic Devices*, NAT'L L. REV. (Jan. 10, 2018), https://www.natlawreview.com/article/cbp-revises-rules-border-searches-electronic-devices [https://perma.cc/MMT2-9UP6]; James Garland & Katharine Goodloe, *Federal Appeals Courts Split on Forensic Searches of Devices Seized at Border*, THE NAT'L L. REV. (May 30, 2018), https://www.natlawreview.com/article/federal-appeals-courts-split-forensic-searches-devices-seized-border [https://perma.cc/9E4T-KP7X].

146. *E.g.*, United States v. Flores-Montano, 541 U.S. 149, 152 (2004) ("The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border.").

147. The Directive cites two examples: "[T]he existence of relevant national security-related lookout in combination with other articulable factors as appropriate, or the presence of an individual on a government-operated and government-vetted terrorist watch list." CBP DIRECTIVE NO. 3340-049A, *supra* note 1, at 5. The first example is arguably just as broad as the terms it is trying to define. The latter example is so specific that it would be hard to surmise analogous situations.

Fourth Amendment doctrines with modern technologies, the courts may be poorly positioned to do so. Justice Samuel Alito has recognized this limitation, advocating instead that legislatures, because they are elected by the people, are in a better position to assess and respond to the rapidly changing role electronic devices have come to play in contemporary life.[148] Other scholars and commentators agree[149]—and so does this Note.

Congress or state legislatures, after assessing the legitimate needs of law enforcement at the border and the privacy interests of electronic device owners, could enact legislation that draws reasonable and clear distinctions based on categories of information or other variables. For example, a statute authorizing suspicionless searches of electronic devices at the border could impose detailed restrictions on the level of detail and type of content allowed to be searched, and cite specific situational factors that would trigger such a search. Law professor and former Department of Justice and Department of Homeland security official, Nathan A. Sales, has suggested a number of potentially beneficial regulations that could be implemented as well.[150] Though the current CBP Directive prohibits Officers from "intentionally us[ing] the device to access information that is solely stored remotely,"[151] this limitation does not provide adequate protection to the mounds of personal—and potentially business—information that individuals frequently store right on the device itself. Moreover, most remote storage "clouds" are set to automatically sync with all of the information contained on cell phones and laptops. Thus, the "solely stored remotely" limitation within the CBP policy seems moot.

One plausible regulation that Sales offers is to put limits on the scope of a search when no criminal activity is initially uncovered.[152] The present state of the law at the border—where, with no particular reason, a Customs agent can order an individual entering or leaving the United States to open and leave behind their digital device for a forensic search

148. "In light of these developments, it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth amendment." Riley v. California, 573 U.S. 373, 408 (2014) (Alito, J., concurring).

149. Flipse, *supra* note 119, at 872; *see* Jennifer Granick, *Protecting Yourself from Suspicionless Searches While Traveling*, ELEC. FRONTIER FOUND. (May 1, 2008), http://www.eff.org/deeplinks/2008/05/protecting-yourselfsuspicionlessyourself-suspicionlessyourselfsuspicionless-searches-while-t [https://perma.cc/M6CY-MCJW] (suggesting that individuals contact their congressional representatives to express disagreement with the current governmental policies).

150. *See* Sales, *supra* note 59, at 1128–32. These include formalizing standards for who border agents choose to search and calling for guidelines in the length of time a search may take.

151. CBP DIRECTIVE NO. 3340-049A, *supra* note 1, at 5.

152. Sales, *supra* note 59, at 1131.

of its data—is not, as the government and defenders of the doctrine contend, currently analogous to other routine inspections of property. If digital information is to ultimately be treated as other forms of property, such as the contents in a suitcase, then the scope of the search should be reduced to an instance where customs agents acting without any suspicion should be able to open laptop computers or cell phones, potentially ask their owners to turn them on, and ensure that those devices are what they seem to be and that they belong to their carriers. In this light, this Note recommends that the Department of Homeland Security and CBP acknowledge that it is possible to perform both a routine and a non-routine search of an electronic device, and better outline the preexisting definitional guidelines of the two categories in revised policies so that federal courts can easily determine when reasonable suspicion or a warrant should be required.

This Note first recommends that CBP revise the names of the two categories its current Directive denotes—basic and advanced searches[153]—in order to parallel the longstanding recognizable dicta that is familiar to the courts: routine and non-routine. Uniformity of these definitional terms across courts and the administrative agencies avoids necessitating any additional layers of interpretation by either party, thus better guaranteeing consistency in application. In drawing those definitional guidelines, the administrative agencies should first more explicitly define a routine search. The current definition of "basic search" is insufficient to provide any guidance to either Officers or courts referring to the policy.[154] A better definition would include listing concrete situations, i.e., a request for the owner to turn on the device and performing a cursory examination of it limited in time and in the presence of the owner.

Such a topical examination of an electronic device should not require reasonable suspicion because it would already be justified by the government's compelling interest in national border security. However, should that limited "routine" search result in the unveiling of any

153. CBP DIRECTIVE NO. 3340-049A, *supra* note 1, at 4–5 (defining "basic" and "advanced" searches).

154. Currently, the CBP ambiguously defines "basic search" as "[a]ny border search of an electronic device that is not an advanced search . . ." *Id.* at 4. The exclusions that the Directive lists—"actions taken to determine if a device functions (e.g., turning a device on and off); or actions taken to determine if physical contraband is concealed within the device itself; or the review of information voluntarily provided by an individual in an electronic format . . ."—would better serve to replace the definition of "routine" searches in the updated policy. *Id.* at 2.

suspicious activity, the scope of the search could then be extended.[155] The updated Directive and any other related policy should elaborate on "articulable factors" the current CBP refers to that would support such reasonable suspicion.[156] In any instance when a hard drive or a cell phone is forensically searched, the search should be categorized as "non-routine," and a warrant should be required to perform that search. Not only would this framework be in accord with preexisting Fourth Amendment principles, but it is well supported by commentators[157] and presumably the public alike, who would then be more appropriately informed of what privacy interests to expect at the border and thus empowered to take personal safeguards.

CONCLUSION

Because of a conflict in the decisions of the U.S. Courts of Appeals on this question, and the importance of its resolution to the enforcement of customs laws, the Supreme Court should adopt this Note's recommended solutions. Not only for the reasoning set forth in the preceding section, but also for broader policy concerns. The job of federal courts is to maintain judicial control over police conduct, and the current "punting" of this issue robs society of a protection that is highly desired and valued by citizens—the protection of information on electronic devices. Leaving this issue unresolved, as the Supreme Court routinely has, leaves potential for an "unfettered dragnet effect that is troublesome."[158] Indeed, it may seem farfetched that a situation would occur where an otherwise law-abiding citizen with no prior record, returning from or traveling abroad, would be subjected to a suspicionless, forensic search of her laptop or cell phone resulting in a criminal charge against her. Perhaps this is why the Supreme Court has stayed silent on

155. The idea that the scope of such a topical search—initially justified at its inception due to it occurring at the border—can be extended by the discovery of something giving rise to a reasonable suspicion that there may be other incriminating evidence is a longstanding Fourth Amendment principle. *See* New Jersey v. T.L.O., 469 U.S. 325, 347 (1985) (holding that the scope of a search can be extended if the initial search yields something to suggest that there may be additional incriminating evidence).

156. For example, in *Cotterman*, the court clarified that "[b]y itself, [defendant's] 1992 conviction for child molestation does not support reasonable suspicion . . . . " United States v. Cotterman, 709 F.3d 952, 965 (9th Cir. 2013). Rather, the court listed that it is one but many factors leading it to conclude reasonable suspicion existed. *Id.* The totality of factors included the TECS alert, password protected files on defendant's laptop, defendant's frequent travel in and out of the country, and confirmation by his passport that he had traveled from Mexico which is highly associated with sex trafficking. *Id.* at 968. Thus, it would be more effective for CBP to actually list "articulable factors" or instead refer to a totality of circumstances analysis.

157. *See* Flipse, *supra* note 119, at 873; Sales, *supra* note 59, at 1124.

158. *Cotterman*, 709 F.3d at 966.

the issue. Yet, given the uniquely intimate nature of the information—as well as the breadth of capacity—stored on electronic devices, it seems unwise to presume that the balance of interests at the border should be automatically tipped in favor of the government like it historically has been. Downplaying the reality that searches of electronic devices seized at the border are particularly offensive and exceptionally damaging to individual privacy interests is to use national security to justify a complete erosion of individual liberties at the border.