Over the Border, Under What Law: The Circuit Split over Searches of Electronic Devices on the Border

Ashley N. Gomez*

"Doublethink means the power of holding two contradictory beliefs in one's mind simultaneously, and accepting both of them."[1]

I. INTRODUCTION

On January 30, 2017, Sidd Bikkannavar arrived at the George Bush Intercontinental Airport in Houston, Texas from a trip to Chile.[2] He had taken a few weeks off from work to go on a personal trip to pursue his hobby of racing solar-powered cars.[3] He is a natural-born U.S. citizen, an employee of a federal agency—NASA's Jet Propulsion Laboratory—and a "seasoned international traveler."[4] After U.S. Custom and Border Protection ("CBP") processed Sidd's passport, a CBP officer detained him and brought him into a separate room within the airport.[5] There, the CBP officer questioned him about where he came from, where he lived, and where he worked.[6] The CBP officers questioned Sidd on information they already possessed through his

* J.D. Candidate, 2020, Sandra Day O'Connor College of Law at Arizona State University; B.A., 2016, University of California, Berkeley. For her advice and guidance on this paper and beyond, I wish to thank Professor Jessica Berch. For always encouraging and supporting me, I would like to thank my parents, Axel and Linda Gomez.

1. GEORGE ORWELL, 1984 214 (First Signet Classics Publishing 1950) (1949).
2. Loren Grush, *A US-Born NASA Scientist Was Detained at the Border Until He Unlocked His Phone*, VERGE (Feb. 12, 2017, 12:37 PM), https://www.theverge.com/2017/2/12/14583124/nasa-sidd-bikkannavar-detained-cbp-phone-search-trump-travel-ban [https://perma.cc/2L7D-344X]; *see also* Hamza Shaban, *Apple Employee Detained by U.S. Customs Agents After Declining to Unlock Phone, Laptop*, WASH. POST (Apr. 3, 2019), https://www.washingtonpost.com/technology/2019/04/03/apple-employee-detained-by-us-customs-agents-after-declining-unlock-phone-laptop/?utm_term=.297f0f10f641 [https://perma.cc/7XAH-KGPJ]; Letter from William S. Freeman et al., ACLU FOUND. N. CAL., to Office of Inspector General, DHS, et al. 3 (Mar. 28, 2019), https://www.aclunc.org/docs/ACLU-NC_2019-03-28_Letter_re._Electronic_Device_Search_SFO.pdf [https://perma.cc/DA6A-HU39].
3. Grush, *supra* note 2.
4. *Id*.
5. *Id*.
6. *Id*.

membership in CBP's "Global Entry" program—an expedited clearance program for "pre-approved, low-risk travelers" returning to the U.S.[7]

Subsequently, the CBP officer asked Sidd to surrender his work-issued cell phone and reveal the phone's passcode.[8] Sidd was told he could not leave the airport until he provided CBP with access to the contents of his cell phone.[9] Eventually, Sidd agreed.[10] The CBP agent subsequently took the cell phone behind closed doors and did not return the cell phone for around thirty minutes.[11] To this day, Sidd has never been told what the CBP agent found on his cell phone or why the agent took possession of his cell phone in the first place.[12]

Due the reach of technology in the United States today, Sidd's story may not be an anomaly.[13] As of 2019, ninety-six percent of U.S. adults owned a cell phone.[14] As Americans spend more time on their electronic devices,[15]

---

7. Julie Travers, *NASA Scientist Detained at Border, Forced To Unlock Phone*, ECOWATCH (Feb. 13, 2017, 11:43 AM), https://www.ecowatch.com/nasa-sidd-bikkannavar-detained-2259068390.html [https://perma.cc/X2JC-BL2Q]. According to CBP's explanation of the program: "Global Entry is a U.S. Customs and Border Protection (CBP) program that allows expedited clearance for pre-approved, low-risk travelers upon arrival in the United States . . . . Travelers must be pre-approved for the Global Entry program. All applicants undergo a rigorous background check and in-person interview before enrollment." *Global Entry*, U.S. CUSTOMS & BORDER PROT. (Dec. 13, 2019), https://www.cbp.gov/travel/trusted-traveler-programs/global-entry [https://perma.cc/3LQL-KK8H].

8. Grush, *supra* note 2.

9. *Id*.

10. *Id*.

11. *Id*.

12. *Id*.

13. After this incident, Sidd became one of eleven plaintiffs in *Alasaad v. Nielsen*, No. 17-CV-11730-DJC, 2019 WL 5899371, at *3 (D. Mass. Nov. 12, 2019). The other plaintiffs in *Alasaad* include a military veteran, journalists, students, an artist, and a business owner. Several of the plaintiffs are Muslims and people of color. For a majority of the plaintiffs, information observed by agents during the searches of their phones was retained. *Id*. at *3. None of the plaintiffs were ever charged with any crime. Alasaad v. McAleenan*: Challenge to Warrantless Phone and Laptop Searches at the U.S. Border*, AM. C.L. UNION (May 10, 2018), https://www.aclu.org/cases/alasaad-v-mcaleenan-challenge-warrantless-phone-and-laptop-searches-us-border?redirect=cases/alasaad-v-nielsen-challenge-warrantless-phone-and-laptop-searches-us-border [https://perma.cc/N7UU-AQQZ].

14. *Mobile Fact Sheet*, PEW RES. CTR. (June 12, 2019), http://www.pewinternet.org/fact-sheet/mobile/ [https://perma.cc/FZG6-ZA95] (stating that eighty-one percent of Americans own a smart phone); *see also Government Data About Searches of International Travelers' Laptops and Personal Electronic Devices*, AM. C.L. UNION, https://www.aclu.org/government-data-about-searches-international-travelers-laptops-and-personal-electronic-devices [https://perma.cc/SUZ2-6RL4] (revealing that between October 2008 and June 2009 cell phones were the most commonly searched electronic devices).

15. In 2015, a study found that "Americans collectively check their smartphones upwards of 8 billion times per day." Lisa Eadicicco, *Americans Check Their Phones 8 Billion Times a Day*,

more data is being created and stored than ever before.[16] In a similar upward trend, CBP has revealed that digital searches of electronic devices on the border have nearly quadrupled since 2015.[17] As disclosed by CBP procedure, a border search of an electronic device will include "an examination of only the information that is resident upon the device and accessible through the device's operating system."[18] Currently, CBP differentiates between the two main types of electronic searches as "basic" and "advanced," which roughly correlate to the "manual" and "forensic"[19] dichotomy referenced in most case law on this subject.[20] This differentiation can more simply be described as the following: "Basic searches are when agents manually search a device by tapping or mousing around a device to open applications or files. Advanced searches are when agents use other devices or software to conduct forensic analysis of the contents of a device."[21]

TIME (Dec. 15, 2015), http://time.com/4147614/smartphone-usage-us-2015/ [https://perma.cc/5XGM-WK4X].

16. The International Data Corporation estimated in 2017 that by the year 2025, the world will be creating 163 zettabytes of data a year. Andrew Cave, *What Will We Do When the World's Data Hits 163 Zettabytes in 2025?*, FORBES (Apr. 13, 2017, 2:22 PM), https://www.forbes.com/sites/andrewcave/2017/04/13/what-will-we-do-when-the-worlds-data-hits-163-zettabytes-in-2025/#6413388f349a [https://perma.cc/4SUP-KUD6].

17. U.S. CUSTOMS & BORDER PROT., CBP RELEASES UPDATED BORDER SEARCH OF ELECTRONIC DEVICE DIRECTIVE AND FY17 STATISTICS (2018), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and [https://perma.cc/H7A2-PXN2]; Kaveh Waddell, *The Steady Rise of Digital Border Searches*, ATLANTIC (Apr. 12, 2017), https://www.theatlantic.com/technology/archive/2017/04/the-steady-rise-of-digital-border-searches/522723/ [https://perma.cc/3A3T-D6H2].

18. U.S. CUSTOMS & BORDER PROT., CBP DIRECTIVE NO. 3340–049A, BORDER SEARCH OF ELECTRONIC DEVICES 4 (2018). Issues relating to searches of the "cloud" are not discussed in this Comment, principally because CBP claims that CBP agents are not allowed to "seek information stored externally or on a 'cloud' linked to the device." Nick Miroff, *U.S. Customs Agents Are Searching More Cellphones—Including Those Belonging to Americans*, WASH. POST (Jan. 5, 2018), https://www.washingtonpost.com/world/national-security/us-customs-agents-are-searching-more-cellphones--including-those-belonging-to-americans/2018/01/05/0a236202-f247-11e7-b3bf-ab90a706e175_story.html?utm_term=.fade0ab06970 [https://perma.cc/JHQ9-SCZC]; *see also* Bhandari, *infra* note 159 ("[E]ven if you move content from your device to a cloud account, an advanced search of your device could still reveal deleted files and metadata.").

19. Due to the fact that most of the case law uses the "manual" and "forensic" phrasing, I will be using these terms throughout this Comment.

20. *See* U.S. CUSTOMS & BORDER PROT., *supra* note 18, at 4–5.

21. Sophia Cope & Aaron Mackey, *New CBP Border Device Search Policy Still Permits Unconstitutional Searches*, ELECTRONIC FRONTIER FOUND. (Jan. 8, 2018), https://www.eff.org/deeplinks/2018/01/new-cbp-border-device-search-policy-still-permits-unconstitutional-searches [https://perma.cc/H5ZC-GV5D]. For a partially redacted figure comparing "manual" and "advanced" searches, see OFFICE OF INSPECTOR GEN., DEP'T OF HOMELAND SEC., CBP'S SEARCHES OF ELECTRONIC DEVICES AT PORTS OF ENTRY 3 (2018).

Recently, CBP released a directive adopting a policy that requires CBP agents to possess "reasonable suspicion," or alternatively "a national security concern," prior to performing an forensic search.[22] Some courts have interpreted this directive as treating forensic searches of electronic devices effectively as "nonroutine border searches . . . [requiring] reasonable suspicion of activity that violates the customs laws or in cases raising national security concerns."[23] Previously, the Court has found that this type of "nonroutine" search is "constitutionally reasonable only if based on individualized suspicion."[24] Other types of "nonroutine" searches include "highly intrusive searches" that implicate significant "dignity and privacy interests" such as strip, body cavity, and involuntary x-ray searches, as well as destructive drilling.[25] However, since the Supreme Court has not yet heard a case involving technology and the border, the Court has not clarified if this type of "nonroutine" analysis would extend further than invasive body searches or destructive drilling.

As of 2019, the U.S. Supreme Court has yet to hear a case regarding the level of suspicion required for electronic device searches on the border. This has left the issue to be developed among the district and appellate courts with increasing regularity.[26] Two conflicting approaches have emerged among the

---

22. U.S. CUSTOMS & BORDER PROT., *supra* note 18, at 5. It is important to note that CBP's directive only applies to CBP and not to other federal agencies.

23. United States v. Kolsuz, 890 F.3d 133, 146 (4th Cir. 2018) (emphasizing, however, that just because the agency adopted these requirements does not make them constitutionally mandated).

24. *Kolsuz*, 890 F.3d at 138 (referencing United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985)). The Supreme Court has previously recognized, as a "nonroutine" border search, a rectal search of an alimentary canal. *Montoya*, 473 U.S. at 531. In *Montoya*, respondent was detained by customs officers for nearly sixteen hours. *Id*. The Supreme Court held that "detention of a traveler at the border, beyond the scope of a routine customs search and inspection, is justified at its inception if customs agents, considering all the facts surrounding the traveler and her trip, reasonably suspect that the traveler" possesses incriminating evidence of criminal activity. *Id*. at 541.

25. United States v. Flores-Montano, 541 U.S. 149, 152, 154 n.2 (2004); *Montoya*, 473 U.S. at 541 n.4.

26. Recently, the Fifth Circuit in *United States v. Molina-Isidoro*, 848 F.3d 287, 289 (5th Cir. 2018), managed to barely avoid the issue by relying on the "good-faith" exception to the exclusionary rule. Similarly, the Seventh Circuit in *United States v. Wanjiku*, 919 F.3d 472 (7th Cir. 2019) reasoned that because the agents reasonably relied on Supreme Court precedent that required no suspicion for non-destructive border searches of property and nothing more than reasonable suspicion for highly intrusive border searches—which the agents had here—it did not need to reach the issue of what level of suspicion is required (if any) for searches of electronic devices on the border. The First Circuit will likely soon be parceling through this issue as the U.S. District Court for the District of Massachusetts recently held that reasonable suspicion was required to conduct border searches travelers' electronic devices. *Alasaad v. Nielsen*, No. 17-CV-

circuits as to the required standard of proof for forensic searches of electronic devices on the border: 1) the Fourth and Ninth Circuits have required "reasonable suspicion" prior to forensic searches in *United States v. Cotterman* and *United States v. Kolsuz*, respectively,[27] and 2) the Eleventh Circuit has required "no suspicion" at all prior to any electronic device search in *United States v. Touset*.[28] Given the contradictory precedent in the circuits, the Supreme Court should hear a case to clarify the law on this issue and resolve the circuit split.

This issue boils down to a direct conflict between the powerful interests protecting the national border and protecting personal privacy. While the Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," those protections have historically been significantly lessened on the U.S. border due to national security concerns.[29] This reduced expectation of privacy on the border is commonly known as the border search exception to the Fourth Amendment and generally allows government agents to search travelers' property when crossing a U.S. port of entry without any individualized suspicion of criminal activity.[30]

However, as technology advances at a rapid rate, the Supreme Court has increasingly added protections to this type of data by adapting the Fourth Amendment to the technological framework of the modern era.[31] In *Riley v. California*, the Court reasoned that absent "more precise guidance from the founding era," the scope of privacy interests at stake must be weighed against government interest.[32] Because cell phones and laptops differ both qualitatively and quantitatively from the types of property envisioned by the founding fathers, the Court has held that officers need a warrant based on probable cause to search digital information on a cell phone seized from an arrested individual.[33] Then again, in *Carpenter v. United States*, the Court emphasized that the unique nature of data obtained from electronic devices implicates a greater invasion of privacy than other types of searches.[34] There,

---

11730-DJC, 2019 WL 5899371, at *3 (D. Mass. Nov. 12, 2019); *see also* United States v. Cano, 934 F.3d 1002 (9th Cir. 2019); United States v. Saboonchi, 990 F.Supp.2d 536, 539 (D. Md. 2014) (holding that "a forensic computer search cannot be performed under the border search doctrine in the absence of reasonable suspicion").

27. *See infra* Part II.C.1.
28. *See infra* Part II.C.2.
29. U.S. CONST. amend. IV; United States v. Ramsey, 431 U.S. 606, 616 (1977).
30. *See infra* Part II.A.2.
31. *See infra* Part II.B.
32. Riley v. California, 573 U.S. 373, 385 (2014).
33. *Id*. at 393, 403.
34. Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

the Court held that the government's acquisition of cell-site location information was a search within the meaning of the Fourth Amendment and therefore, similar to *Riley*, required a warrant based on probable cause.[35]

The strength of the policy interests behind the two approaches further exacerbates the necessity of resolving the circuit split.[36] The need for a "no suspicion" standard is understandable when assessing the general heightened interest in giving the government the appropriate tools to combat crime at the border.[37] Alternatively, the need for a "reasonable suspicion" standard is understandable when assessing the invasion of individual privacy that occurs when a forensic search of an electronic device is performed at the border.[38] This is specifically apparent when considering the vast amount of information contained on electronic devices and the prevalence of electronic devices among travelers.[39] Additionally, privacy proponents argue that examinations of phones, hard drives, and computers violate the sanctity of the Fourth Amendment's protection against unreasonable searches and seizures when performed without a warrant.[40] Until the Supreme Court clarifies the extent to which the Fourth Amendment protects electronic devices on the U.S. border, both CBP agents and travelers are left in a purgatory of uncertainty.

Section A of Part II provides a brief overview of the Fourth Amendment and the border search exception. Section B highlights a line of decisions by the Supreme Court that suggests that the Fourth Amendment extends specific protections to cover the unique characteristics of technology. Section C follows the history and creation of the current circuit split, from the Ninth Circuit in *Cotterman* to the Eleventh Circuit in *Touset*. Section D continues by addressing the strong policy interests and concerns on both sides of the debate to illustrate the complicated nature that hinders any attempt to craft a bright-line rule. Next, Section E details the possible approaches the Supreme Court may choose from when deciding this issue. Part III argues why the "reasonable suspicion" standard is the most logical choice for forensic searches at the border. Finally, Part IV asserts that following the Court's reasoning in *Carpenter* and *Riley*, which emphatically conveys that searches of electronic devices are fundamentally different from other searches, the circuit split should be decided in favor of the Fourth and Ninth Circuits to

35. *Id*. at 2220–21.
36. *See infra* Part II.D.
37. *See infra* Part II.D.1.
38. *See infra* Part II.D.2.
39. *See infra* Part II.D.2.
40. *See* Ron Nixon, *Cellphone and Computer Searches at U.S. Border Rise Under Trump*, N.Y. TIMES (Jan. 5, 2018), https://www.nytimes.com/2018/01/05/us/politics/trump-border-search-cellphone-computer.html [https://perma.cc/53Q7-E897].

conclude that governmental officials need at least "reasonable suspicion" to conduct forensic searches of electronics on the border.

II. BACKGROUND

The clash between the need for individual privacy and the need for national security inevitably creates sharp divisions in the Fourth Amendment's protective sphere. As technology has become more integrated into the fabric of modern society, the traditional scope of the Fourth Amendment and the border search exception may no longer prove to adequately protect citizens from unreasonable searches and seizures. Section A begins with a brief overview of the Fourth Amendment and the border search exception. Section B addresses the Supreme Court's apparent expansion of the Fourth Amendment's protection to technological property in *Carpenter v. United States* and *Riley v. California*. Section C describes the current circuit split between the Fourth and Ninth Circuits and the Eleventh Circuit regarding the level of suspicion required for searches of electronic devices on the U.S. border. Next, Section D discusses the battle between the conflicting policy justifications supporting each side of the circuit split. Finally, Section E summarizes the possible solutions the Supreme Court could utilize when resolving this discrepancy between circuits.

A. The Fourth Amendment and the Border Search Exception

Throughout U.S. history, the Fourth Amendment has been a foundational source of protection for citizens against unreasonable searches and seizures by the government.[41] The Fourth Amendment, which was established in the Bill of Rights, added guarantees of personal rights to the U.S. Constitution.[42] Throughout Fourth Amendment jurisprudence, the Supreme Court has found many exceptions to the typical requirement of obtaining a warrant based on probable cause from a magistrate judge.[43] One of these exceptions, the border search exception, grants government officials the ability to perform searches of individuals and their effects at U.S. borders without a warrant.[44] With the changing landscape of national security tactics and the unique qualities electronic devices possess, the question of how electronic devices and border

41. U.S. CONST. amend. IV.
42. U.S. CONST. amends. I–X.
43. *See infra* note 168.
44. United States v. Ramsey, 431 U.S. 606, 616 (1977); *see also* Christine A. Coletta, *Laptop Searches at the United States Borders and the Border Search Exception to the Fourth Amendment*, 48 B.C. L. REV. 971, 978 (2007).

searches should be reconciled with the Fourth Amendment has been an issue for scholars and courtrooms alike.[45]

1. The Fourth Amendment

The plain text of the Fourth Amendment can generally be broken up into two main parts—the "reasonableness" clause and the "warrants" clause.[46] The interplay and significance of each portion of the text is a controversial feature in Fourth Amendment jurisprudence.[47] The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[48]

First, this language requires that all searches and seizures be reasonable.[49] This is sometimes referred to as the "reasonableness" clause.[50] Reasonableness is generally determined by looking at all the circumstances surrounding a search or seizure and the nature of the search or seizure.[51] The permissibility of a particular law enforcement practice is judged by "balancing its intrusion on the individual's Fourth Amendment interests

---

45. *See, e.g.*, United States v. Romm, 455 F.3d 990 (9th Cir. 2006); United States v. Ickes, 393 F.3d 501 (4th Cir. 2005); Patrick E. Corbett, *The Future of the Fourth Amendment in a Digital Evidence Context: Where Would the Supreme Court Draw the Electronic Line at the International Border?*, 81 MISS. L.J. 1263, 1264–66 (2012); Benjamin J. Rankin, *Restoring Privacy at the Border: Extending the Reasonable Suspicion Standard for Laptop Border Searches*, 43 COLUM. HUM. RTS. L. REV. 301, 301–05 (2011).

46. Kentucky v. King, 563 U.S. 452, 459 (2011); Thomas K. Clancy, *The Fourth Amendment's Concept of Reasonableness*, 2004 UTAH L. REV. 977, 993 (2004).

47. *See* JOSHUA DRESSLER & GEORGE C. THOMAS III, CRIMINAL PROCEDURE 71–72 (6th ed. 2016). The authors address some of the prominent questions regarding this issue, such as:

> Does the warrant clause mean that searches conducted without warrants are (at least, presumptively) unreasonable, and, consequently, in violation of the reasonableness requirement? Or did the drafters of the Fourth Amendment mean only that *when* a warrant is issued it must meet the requirements of probable cause, oath or affirmation, and particularity, but that there is no warrant requirement, as such?

Id.

48. U.S. CONST. amend. IV.

49. *King*, 563 U.S. at 459.

50. Clancy, *supra* note 46, at 993.

51. United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985).

against its promotion of legitimate governmental interests."[52] Second, if law enforcement does obtain a warrant prior to a search or seizure, the warrant must be based on probable cause.[53] This is sometimes referred to as the "warrants" clause.[54] Possession of a warrant to perform a search or seizure is presumptively reasonable, unless some deficiency is found.[55]

2. The Border Search Exception

One exception to the Fourth Amendment's stringent warrant requirement is the border search exception. The border search exception is rooted in the "long-standing right of the [government] to protect itself by stopping and examining persons and property crossing into this country."[56] Searches do not necessarily need to occur at an international border itself but can occur at its "functional equivalent"—namely, any port of entry.[57] Courts have generally accepted that the rationales underlying the border search exception extend equally to both entry and exit searches.[58] Because of the unique circumstances of the border, courts have long considered border searches as an "historically recognized exception to the Fourth Amendment's general principle that a warrant be obtained."[59]

---

52. Delaware v. Prouse, 440 U.S. 648, 654 (1979).

53. *See King*, 563 U.S. at 459.

54. Clancy, *supra* note 46, at 993.

55. *See, e.g.*, Lo-Ji Sales, Inc. v. New York, 442 U.S. 319, 325–26, 329 (reversing a conviction based on a search warrant where the issuing judge was not neutral and detached and the warrant did not describe with particularity the things to be seized).

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

57. Almeida-Sanchez v. United States, 413 U.S. 266, 272–73 (1973) (noting that searches at an established station near the border or passengers and cargo on an international flight landing in the United States might be the functional equivalent of a border search); *see* 8 U.S.C. § 1357(a)(3) (2018) (allowing CBP officials the authority to stop and conduct searches on any train, aircraft, conveyance, or vehicle within a "reasonable distance from any external boundary of the United States"); 8 C.F.R. § 287.1(a)(2) (2020) (defining "reasonable distance" as "100 air miles from any external boundary of the United States"); *see also* Chris Rickerd, *ACLU Factsheet on Customs and Border Protection's 100-Mile Zone*, AM. C.L. UNION, https://www.aclu.org/other/aclu-factsheet-customs-and-border-protections-100-mile-zone?redirect=immigrants-rights/aclu-fact-sheet-customs-and-border-protections-100-mile-zone [https://perma.cc/86S3-EFRM] ("Allowing CBP to divert its attention from the border distracts from its primary mission and results in widespread violations of Americans' rights to property and liberty, including Fourth Amendment and other constitutional violations." (emphasis omitted)).

58. *See, e.g.*, United States v. Oriakhi, 57 F.3d 1290, 1296–97 (4th Cir. 1995); United States v. Ezeiruaku, 936 F.2d 136, 143 (3d Cir. 1991).

59. *Ramsey*, 431 U.S. at 621.

However, courts typically maintain that warrantless searches must still be reasonable regardless of the proximity to the border.[60] The reasonableness of the search or seizure is based on the totality of the circumstances.[61] This includes examining whether the scope and duration of the search or seizure is reasonable.[62] However, due to the government's heightened interest in preventing illicit persons and property from entering the country, border searches are generally deemed "reasonable simply by virtue of the fact that they occur at the border."[63] Even so, an individual's privacy rights must still be balanced against the government's interests when determining reasonableness.[64] After conducting this balancing test, the Supreme Court has found as permissible—without reasonable suspicion, probable cause, or a warrant—searches on the border of luggage, mail, and persons[65] as well as the dismantlement of a motor vehicle.[66]

B. The Supreme Court's Recent Jurisprudence Regarding the Fourth Amendment and Electronic Devices

As technology has rapidly advanced, the Fourth Amendment has seemingly been pulled in opposite directions.[67] The landmark and unanimous decision in *Riley v. California*—which held that, during an arrest, warrantless searches and seizures of a cell phone's digital content are unconstitutional—indicated the Court's awareness of the role technology plays in modern

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

61. United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985).

62. *Id*.; *see also Cotterman*, 709 F.3d at 963.

63. *Ramsey*, 431 U.S. at 616.

64. *Montoya*, 473 U.S. at 539. While an individual's privacy must be weighed against the government's interest in protecting international borders, the balance is "struck much more favorably to the Government." *Id*. at 540.

65. *Id*. at 538.

66. United States v. Flores-Montano, 541 U.S. 149, 155–56 (2004).

67. *See also* Kyllo v. United States, 533 U.S. 27, 33–34 (2001) ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has not been entirely unaffected by the advance of technology . . . . The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy."); Judge Herbert B. Dixon Jr., *Telephone Technology Versus the Fourth Amendment*, 55 JUDGES' JOURNAL 37 (2016), https://www.americanbar.org/groups/judicial/publications/judges_journal/2016/spring/telephone_technology_versus_the_fourth_amendment/ [https://perma.cc/6GCX-GME6] ("When it comes to addressing any Fourth Amendment issue related to the rapid advancements in . . . technology, to ask what the framers intended might be aptly described as a foray into the twilight zone.").

society's understanding of "reasonableness."[68] A few years later, the Supreme Court approached this tension between technology and the Fourth Amendment again in *Carpenter v. United States*.[69] Building on *Riley*, the Court recognized that the traditional rationales for allowing warrantless searches under Fourth Amendment jurisprudence may not be appropriate for electronic devices.[70] Together, both decisions seemingly create a carve-out within Fourth Amendment jurisprudence that indicates that technology is inherently different from other types of property and therefore may require different protections.[71]

1. *Riley v. California* (2014)

In *Riley v. California*, the Supreme Court held that the police may not, without a warrant, search or seize the digital information on a cell phone of an arrested individual.[72] Recognizing the inherent role that technology plays in modern society, the Court framed this issue as how the search-incident-to-arrest doctrine[73] applied to "to modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[74] "Modern cell phones," as the Court emphasized, "are not just another technological convenience."[75] After clarifying that law enforcement officers still remain free to examine the physical aspects of a cell phone to establish that it cannot be used as a weapon, the Court rejected the government's

---

68. *See* Paul Ohm, *The Life of* Riley *(*v. California*)*, 48 TEX. TECH L. REV. 133, 134 (2015) (arguing that *Riley* did "much more" than establish a narrow holding regarding arrests but was instead a "paean to privacy in the modern, technological era"); Kristen J. Mathews, *Landmark Supreme Court Ruling Protects Cell Phones from Warrantless Searches*, NAT'L L. REV. (June 30, 2014), https://www.natlawreview.com/article/landmark-supreme-court-ruling-protects-cell-phones-warrantless-searches [https://perma.cc/4D97-BJDJ].

69. 138 S. Ct. 2206 (2018).

70. *Id*. at 2214.

71. *See, e.g*., Louise Matsakis, *The Supreme Court Just Greatly Strengthened Digital Privacy*, WIRED (June 22, 2018, 12:26 PM), https://www.wired.com/story/carpenter-v-united-states-supreme-court-digital-privacy/ [https://perma.cc/9GHH-E2V6].

72. Riley v. California, 573 U.S. 373, 386–87, 403 (2014).

73. The search-incident-to-arrest doctrine—which developed from common law—allows governmental agents to search an arrestee without a warrant pursuant to a lawful arrest. Weeks v. United States, 232 U.S. 383, 392 (1914). However, the scope of the search has been the subject of case law. *See, e.g*., United States v. Robinson, 414 U.S. 218, 235 (1973); Chimel v. California, 395 U.S. 752, 762–63 (1969); Terry v. Ohio, 392 U.S. 1, 16 (1968).

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

75. *Id*. at 403.

arguments that searching cell phone data was necessary to ensure officer safety and prevent destruction of evidence prior to obtaining a warrant.[76]

In the consolidated case of *Riley*, after the lawful arrests of Riley and Wurie, law enforcement agents accessed incriminating data from the arrestees' phones without first obtaining a warrant.[77] Under the search-incident-to-arrest doctrine, officers are generally allowed to search the area within the arrestee's possession or control.[78] Under this exception, the Court had previously allowed for searches of containers on lawfully arrested persons.[79] Although a cell phone has many similarities to computers, the *Riley* Court focused specifically on the unique qualities of a cell phone since that was the technology at issue in the case.[80]

The *Riley* Court emphasized that cell phones differ in both a "quantitative and a qualitative sense from other objects."[81] Quantitatively, the Court noted that cell phones have an immense storage capacity, which has the ability to store a vast amount of information.[82] The Court reasoned with a proportionality argument:

> Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so. And if they did, they would have to drag

76. *Id*. at 386–90.

77. *Id*. at 378–81.

78. *Chimel*, 395 U.S. at 763–65.

79. *See, e.g*., United States v. Robinson, 414 U.S. 218, 236 (1973) (permitting the search inside of a cigarette package that was found inside Robinson's coat pocket after he was lawfully arrested).

80. *Riley*, 573 U.S. at 385–86.

81. *Id*. at 393 (noting that these "minicomputers" could easily be called "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers").

82. *Id*. at 393. The Court continued by emphasizing the large storage capacity of the current top-selling smart phone in 2014, which could hold a minimum of sixteen gigabytes or a maximum of sixty-four gigabytes. *Id*. at 394. According to the Court, sixteen gigabytes translates into "millions of pages of text, thousands of pictures, or hundreds of videos," which has serious consequences for the owner's privacy if that information is obtained. *Id*. However, the newest models in Apple's iPhone series (iPhone 11 Pro and iPhone 11 Pro Max) now possess a minimum storage capacity of sixty-four gigabytes or a maximum storage capacity of 512 gigabytes, greatly widening the amount of possible information contained on a cell phone and possible privacy concerns. *iPhone 11 Pro*, APPLE INC., https://www.apple.com/iphone-11-pro/specs/ [https://perma.cc/E5P8-WVPW]; s*ee also* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 542 (2005) (stating that eighty gigabytes equals roughly forty million pages of text or the amount of information contained in books filling an entire floor of a typical academic library).

> behind them a trunk of the sort held to require a search warrant . . . .[83]

Qualitatively, the Court reasoned that cell phones reveal a breadth of information about an individual's interests, concerns, and locations.[84] This led the Court to conclude that a search of a cell phone would expose "far more than the most exhaustive search of a house," a location explicitly protected by the Fourth Amendment.[85] Thus, the Court directly emphasized that the diminished privacy rights a person possesses in a specific situation—here, a search incident to arrest—does not mean the Fourth Amendment "falls out of the picture entirely."[86]

2. *United States v. Carpenter* (2018)

Four years after *Riley*, the Supreme Court heard another case involving electronic devices and the Fourth Amendment in *United States v. Carpenter*.[87] The Supreme Court held that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through cell-site location information ("CSLI").[88] The Court emphasized that the basic purpose of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."[89] Particularly, the Court reasoned that "[a]s technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure[] preservation of that degree of privacy against government that existed when

---

83. *Riley*, 572 U.S. at 393–94.

84. *Id.* at 395–96.

85. *Id.* at 396–97 (reasoning that "[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").

86. *Id.* at 392.

87. Interestingly, while Chief Justice Roberts delivers the opinion in both *Riley* and *Carpenter*, the unanimous decision in *Riley* is followed by a 5–4 split in *Carpenter*.

88. Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018). The Court explains what cell-site location information is:

> Cell phones continuously scan their environment looking for the best signal, which generally comes from the closest cell site. Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI).

Id. at 2211.

89. *Id*. at 2213 (internal quotation marks omitted) (quoting Camara v. Mun. Court of City & Cty. of S.F., 387 U.S. 523, 528 (1967)).

the Fourth Amendment was adopted.'"[90] Building on the *Riley* decision, the Court foreshadowed its analysis by emphasizing, once again, that due to the immense storage capacity and types of sensitive information embedded on cell phones, this type of property differs in both a quantitative and qualitative sense from other types of property.[91]

After recognizing that individuals have a reasonable expectation of privacy in their movements, the Court refused to extend the third-party doctrine[92]—which generally allows searches or seizures without any suspicion required—to apply to the facts of *Carpenter*.[93] Similar to the GPS information deemed private in previous decisions,[94] the CSLI data provided "an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[95] The Court continued by stating that cell phones achieve "near perfect surveillance."[96] As a word of caution to future Fourth Amendment jurisprudence, the Court quoted Justice Brandeis' famous dissent: "the Court is obligated—as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government'—to ensure that the 'progress of science' does not erode Fourth Amendment protections."[97]

---

90. *Id*. at 2214 (alteration in original) (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)); *see also Kyllo*, 533 U.S. at 34 (concluding that law enforcement could not capitalize on such new sense-enhancing technology to discover what was occurring within the home without obtaining a warrant).

91. *See Carpenter*, 138 S. Ct. at 2214.

92. Stemming from the decisions of *Smith v. Maryland* and *United States v. Miller*, the third-party doctrine allows the government to access information citizens voluntarily provide to third parties without violating the Fourth Amendment. Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 442 (1976).

93. *Carpenter*, 138 S. Ct. at 2215–17 (declining to extend *Smith v. Maryland* and *United States v. Miller* to cover digital information obtained through cell-site location information).

94. *See, e.g.*, United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). In *Jones*, the Court held that the government's attachment of a GPS device to the undercarriage of a car and its use of the GPS device to monitor Jones' movements, constituted an unconstitutional search under the Fourth Amendment. *Id*. at 404–05 (majority opinion).

95. *Carpenter*, 138 S. Ct. at 2217 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).

96. *Id*. at 2218. The Court stressed how invasive cell phone data can be: "A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Id*.

97. *Id*. at 2223 (quoting Olmstead v. United States, 277 U.S. 438, 473–74 (1928)).

C. *Case History of the Circuit Split: From* Cotterman *to* Touset

As technology becomes a more pervasive part of modern culture, the clash between border protection and invasive forensic searches has led to different results among the circuits on how to deal with emerging technologies, cybersecurity, and border protection. The crux of the current circuit split is whether a "no suspicion" standard satisfies the Fourth Amendment—supported by the Eleventh Circuit in *United States v. Touset*[98]—or whether, at least, a "reasonable suspicion" standard is required—supported by the Ninth and Fourth Circuits in *United States v. Cotterman* and *United States v. Kolsuz*, respectively.[99]

1. The "Reasonable Suspicion" Standard: The Ninth and Fourth Circuits

a. United States v. Cotterman *(2013)*[100]

In *United States v. Cotterman*, the Ninth Circuit en banc held that "reasonable suspicion" was required for the forensic examination[101] of the defendant's computer after he had presented it for inspection at the U.S. border.[102] After an initial, basic search revealed no evidence of wrongdoing,

---

98. United States v. Touset, 890 F.3d 1227, 1234–35 (11th Cir. 2018).

99. United States v. Kolsuz, 890 F.3d 133, 145–46 (4th Cir. 2018); United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013); *see also* United States v. Cano, 934 F.3d 1002 (9th Cir. 2019).

100. This case was presented before Chief Judge Kozinski, Judge Thomas, Judge McKeown, Judge Wardlaw, Judge Fisher, Judge Gould, Judge Clifton, Judge Callahan, Judge Smith, Judge Murguia, and Judge Christen. *Cotterman*, 709 F.3d at 956. Judge McKeown wrote the opinion for the court. *Id*.

101. *See supra* notes 19–21 and accompanying text. Recently, the Ninth Circuit in *United States v. Cano* clarified its holding in *Cotterman*. United States v. Cano, 934 F.3d 1002 (9th Cir. 2019). First, the court affirmed that "manual cell phone searches may be conducted by border officials without reasonable suspicion but that *forensic* cell phone searches require reasonable suspicion." *Id*. at 1007. Then, the court held that reasonable suspicion in this context means that "officials must reasonably suspect that the cell phone contains digital contraband." *Id*. Finally, the court concluded that "cell phone searches at the border, whether manual or forensic, must be limited in scope to a search for digital contraband." *Id*. While the court noted that it agreed with much of the *Kolsuz* decision's discussion of foundational principles, it disagreed on the proper scope of a forensic border search. *Id*. at 1018. Specifically, the Ninth Circuit emphasized that border agents cannot "conduct a warrantless search for evidence of past or future border-related crimes"—this is a further protection from *Kolsuz* which approved forensic searches for further evidence of ongoing crimes. *Id*. at 1017–18.

102. *Cotterman*, 709 F.3d at 957. Previously, in a case on the same issue, the Ninth Circuit reasoned that simply because border searches are generally deemed reasonable by their

CBP seized the defendant's laptop and conducted a forensic search days later and 170 miles away from the border.[103] The initial search of Cotterman's laptop was not at issue since the court had previously found that a suspicionless "quick look" of a laptop is reasonable.[104] Before delving into its analysis, the court rejected the government's argument that a forensic examination of Cotterman's computer constituted an "extended border search."[105] The Ninth Circuit clarified that it is the "comprehensive and intrusive nature" of the search and not the location of the search that triggers the need for "reasonable suspicion."[106] While Cotterman's expectation of privacy was diminished on the border, a person's "'dignity and privacy interests' . . . will on occasion demand 'some level of suspicion in the case of highly intrusive searches.'"[107]

The Ninth Circuit then proceeded by depicting the data stored on electronic devices as falling under the Fourth Amendment's protection of "papers."[108] Proportionally, the storage capacity and types of sensitive information contained on electronic devices greatly outweigh the amount and type of information that could be discovered in luggage.[109] To the court, while it was reasonable to expect citizens would remove property they did not want searched from their luggage before traveling, it was clearly unreasonable to expect citizens to remove sensitive information from electronic devices: "When carrying a laptop, tablet or other device . . . removing files unnecessary to an impending trip is an impractical solution given the volume and often intermingled nature of the files."[110]

However, the Ninth Circuit found that electronic devices were not immune to *all* searches at the border.[111] Rather, determining whether a search will violate the Fourth Amendment was a question of reasonableness—which,

---

occurrence at the border does not mean that "anything goes." United States v. Seljan, 547 F.3d 993, 999–1000 (9th Cir. 2008) (noting that while the Supreme Court has suggested that the Fourth Amendment places "some limits on searches at the border," the Court has "neither spoken definitively on that subject nor clearly defined the limits").

103. *Cotterman*, 709 F.3d at 958.

104. *Id*. at 960 (referencing United States v. Arnold, 533 F.3d 1003, 1009 (9th Cir. 2008)).

105. *Id*. at 961–62.

106. *Id*. at 962.

107. *Id*. at 963 (quoting United States v. Flores-Montano, 541 U.S. 149, 152 (2004)). The Ninth Circuit also notes that some border searches are so "overly intrusive" that they require "particularized suspicion." *Id*.

108. *Id*. at 964.

109. *Id*. at 964–65 ("Even a car full of packed suitcases with sensitive documents cannot hold a candle to the sheer, and ever-increasing, capacity of digital storage.").

110. *Id*. at 965.

111. *Id*. at 966.

"must account for differences in property."[112] The court reasoned that due to the unique qualities of electronic devices, an exhaustive forensic search of an electronic device was inherently more intrusive than a search of other forms of property.[113] While there were obviously important security concerns at the border, there were also heightened Fourth Amendment and privacy concerns for travelers.[114] Thus, the Ninth Circuit concluded that "reasonable suspicion" was required for the forensic search of Cotterman's computer.[115]

b. United States v. Kolsuz *(2018)*[116]

Following the position enunciated in *Cotterman*, the Fourth Circuit in *United States v. Kolsuz* upheld the district court's conclusion that "under *Riley*, the forensic examination of Kolsuz's phone must be considered a nonroutine border search, requiring some measure of individualized suspicion."[117] After CBP arrested Kolsuz for possession of firearms, CBP agents seized Kolsuz's smartphone and subjected it to a month-long, off-site forensic analysis that produced a 896-page report.[118] The district court had previously concluded that the original "manual search"[119] of Kolsuz's cell phone was a routine border search whereas the forensic search constituted a nonroutine search.[120] The district court reasoned that a smartphone cannot

---

112. *Id*.

113. *Id*. at 965–66.

114. *Id*. at 966.

115. *Id*. at 967–68. However, the court determined that the agents' examination of the computer was supported by reasonable suspicion. *Id*. at 970.

116. This case was presented before Judge Wilkinson, Judge Motz, and Judge Harris. United States v. Kolsuz, 890 F.3d 133, 135 (4th Cir. 2018).

117. *Id*. at 137. Additionally, the court reserved the question of whether the reasonable suspicion standard was enough or whether a warrant based on probable cause was required. *Id*. Following its decision in *Kolsuz*, the Fourth Circuit recently held that a warrantless forensic search of an airline passenger's electronic devices was not justified under the border search exception. United States v. Aigbekaen, 943 F.3d 713, 721–23 (4th Cir. 2019). However, while finding a constitutional violation had occurred, the court found that the evidence did not have to be suppressed given the agents' "good-faith" reliance on the existing precedent prior to the *Kolsuz* decision. *Id*. at 725.

118. *Id*. at 138–39 (finding that the report included Kolsuz's "personal contact lists, emails, messenger conversations, photographs, videos, calendar, web browsing history, and call logs, along with a history of Kolsuz's physical location down to precise GPS coordinates").

119. *See supra* notes 19–21 and accompanying text.

120. *Kolsuz*, 890 F.3d at 140. While the Fourth Circuit did not explicitly define the difference between a "manual" and "forensic" search, the court acknowledged that in *United States v. Ickes*, the Fourth Circuit "treated as routine a border inspection of a computer's contents, accessed *manually* 'in the same way a typical user would' and without any 'sophisticated *forensic* analysis.'" *Id*. (emphasis added) (quoting United States v. Kolsuz, 185 F. Supp. 3d 843, 853 (E.D. Va. 2016); *see also* H. MARSHALL JARRETT ET AL., SEARCHING AND SEIZING COMPUTERS AND

simply be analogized to a normal piece of luggage, but it was more aptly comparable to a "body cavity search."[121]

The Fourth Circuit acknowledged that even before the Supreme Court's decision in *Riley*, courts supported recognizing forensic searches of electronic devices as nonroutine.[122] Specifically, the immense storage capacity, the sensitivity of the information, and the inability to efficiently mitigate the information held on electronic devices separated electronic devices from other types of property that were typically subject to suspicion-free searches on the border.[123] In the court's view, *Riley* merely confirmed this assessment: "[t]he key to *Riley*'s reasoning is its express refusal to treat such phones as just another form of container."[124] Therefore, the Fourth Circuit found that after the holding in *Riley*, the Fourth Amendment required law enforcement to meet a "reasonable suspicion" standard when performing forensic searches under the border search exception.[125]

2. The "No Suspicion" Standard: The Eleventh Circuit

a. United States v. Touset *(2018)*[126]

Less than a week after the *Kolsuz* decision, the Eleventh Circuit in *United States v. Touset* directly rejected the decisions of the Ninth and Fourth Circuits and held that "reasonable suspicion" is *never* required for searches of electronic devices on the border.[127] Specifically, the court denied the defendant's Motion to Suppress the child pornography images found on his electronic devices during a border inspection because it found that either "no suspicion" was required for electronic searches on the border or, alternatively, that CBP had "reasonable suspicion" to search Touset.[128] In a decision by the Eleventh Circuit roughly two months earlier, the court in

---

OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 86–87 (2009) (providing an example of the process of a two-stage forensic analysis search).

121. *Kolsuz*, 890 F.3d at 140 (quoting United States v. Saboonchi, 990 F. Supp. 2d 536, 569 (D. Md. 2014)).

122. *Id*. at 144.

123. *Id*. at 145.

124. *Id*.

125. From the factual finding of the lower courts, CBP had met this standard. *Id*. at 146–47.

126. This case was presented before Judge Pryor, Judge Carnes, and Judge Corrigan. United States v. Touset, 890 F.3d 1227, 1229 (11th Cir. 2018).

127. *Id*.

128. *Id*.

United States v. Vergara had held that the Fourth Amendment did not require a warrant or probable cause to search a cell phone on the border.[129]

The *Touset* court interpreted *Vergara* and other laws and precedent as making clear that "no suspicion is necessary to search electronic devices on the border."[130] Conducting a historical analysis of the Fourth Amendment, the court maintained that the First Congress "empowered" customs officials to search individuals "illegally entering" the U.S. without a warrant, which therefore supported the perspective that warrants are never required for border searches.[131] Additionally, because the Supreme Court has never explicitly required "reasonable suspicion" for the search of property at the border, the Eleventh Circuit reasoned it should therefore not create any exceptions for electronic devices.[132] Following this reasoning, the court concluded that electronic devices should not receive "special treatment" simply due to the fact that many people own them and that they can store vast amounts of information.[133]

While acknowledging the decisions of the Ninth and Fourth Circuits that required "reasonable suspicion" for forensic searches of electronic devices on the border, the Eleventh Circuit stated it was "unpersuaded."[134] The Eleventh Circuit was unpersuaded on three grounds.[135] First, drawing on its holding in *Vergara*, *Riley* applied only to searches incident to arrest, not border searches.[136] Second, the Eleventh Circuit's precedent only has considered the "'personal indignity' of a search, not its extensiveness."[137]

---

129. United States v. Vergara, 884 F.3d 1309, 1311 (11th Cir. 2018). The defendant argued that following *Riley*, law enforcement agents must obtain a warrant based on probable cause before conducting a forensic search of electronic devices. *Id*. However, the court concluded that *Riley* solely applies to the search-incident-to-arrest exception. *Id*. at 1312. The Eleventh Circuit reasoned that "border searches 'never' require probable cause or a warrant"—with the exception of highly intrusive searches of the body—and therefore the Fourth Amendment does not require a warrant or probable cause for forensic searches on the border. *Id*. The court declined to address whether reasonable suspicion is required for all electronic searches at the border but claimed that reasonable suspicion would be the highest standard for such a search. *Id*. at 1313.

130. *Touset*, 890 F.3d at 1229.

131. *Id*. at 1232; *see* Act of July 31, 1789, ch. 5, §24, 1 Stat. 29, 43 (granting customs officials "full power and authority" to enter and search "any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed").

132. *Touset*, 890 F.3d at 1233. The Eleventh Circuit reasoned that since it had upheld a search of a ship cabin without reasonable suspicion and a cabin is more like a home, which receives the most stringent Fourth Amendment protections, that there is no reason to require reasonable suspicion for forensic searches of electronic devices. *Id*.

133. *Id*. at 1233.

134. *Id*. at 1234.

135. *Id*.

136. *Id*.

137. *Id*.

Third, a traveler's interest in privacy should not be given a greater weight than the government's interest in protecting the nation.[138] Emphasizing this point, the court explained that since travelers are on notice that they may be searched, "they are free to leave any [electronic devices] they do not want searched—unlike their bodies—at home."[139] Allowing this protection for electronic devices undermined the government's interest in stopping contraband and would only create a "special protection" to benefit criminals.[140] Finally, the Eleventh Circuit concluded that Congress, not the judicial branch, was in the best position to determine the appropriate standard for forensic searches of electronic devices on the border. [141]

D. Clash of the Titans: National Security Versus Individual Privacy

The Court in *Riley v. California* noted that since the founding era does not provide much guidance for dealing with technology, the Court must weigh this idiosyncrasy in Fourth Amendment jurisprudence by assessing the "degree to which [the search and seizure] intrudes upon an individual's privacy and . . . the degree to which it is needed for the promotion of legitimate governmental interests."[142] The U.S. government and national security proponents emphasize that electronic device searches are essential to "protect the homeland, enforce the law at our borders, and follow [the government's] oath to uphold [the] Constitution" and therefore do not require stricter protections.[143] Alternatively, privacy proponents stress that because of the unique characteristics of electronic devices, electronic device searches at the border—regardless of the extent of the search—are "extremely invasive" and therefore require stricter protections.[144]

1. National Security Interests

On one side, government officials possess a broad discretion to search any media player or communication, electronic, or digital device at the border

---

138. *Id*. at 1235.
139. *Id*.
140. *Id*. at 1235–36.
141. *Id*. at 1236–37.
142. Riley v. California, 573 U.S. 373, 385 (2014) (internal quotation marks omitted) (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).
143. Joseph B. Maher, *DHS: Device Searches Improve Safety*, USA TODAY (Mar. 27, 2017, 2:57 PM), https://www.usatoday.com/story/opinion/2017/03/27/dhs-device-searches-improve-safety-editorials-debates/99697022/ [https://perma.cc/QY7A-A736].
144. Miroff, *supra* note 18.

under both judicial precedent and statutory authority.[145] This broad authority at the border is premised on the need "to protect the American people and enforce the nation's laws in this digital age."[146] This protection of the nation includes, but is not limited to, the detection of terrorist activity, human smuggling, and child pornography.[147] According to CBP, only a "small number of travelers" have their devices searched—specifically, the number equates to fewer "than one-hundredth of 1 percent of all arriving international travelers."[148] Although recognizing the increasing number of electronic devices searched each year, CBP claims this escalation is simply due to more travelers carrying electronic devices.[149]

National security advocates highlight that without a robust border security policy in place "terrorist or other international criminals could use laptops as a means to smuggle messages and plans into the country for distribution to cells and allies."[150] Further, the Federal Bureau of Investigation asserts that "cyber intrusions are becoming more commonplace, more dangerous, and more sophisticated."[151] Fears that crime is transpiring on the border also seem necessarily justified by the fact that most of the border search exception jurisprudence is based on people who have actually committed a crime and are trying to suppress the incriminating evidence that was found on their electronic device.[152] Thus, the argument that the further diminishment of the CBP's broad authority on the border would result in

---

145. U.S. CUSTOMS & BORDER PROT., *supra* note 18, at 1, 4.

146. U.S. CUSTOMS & BORDER PROT., CBP RELEASES STATISTICS ON ELECTRONIC DEVICE SEARCHES (2017), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0 [https://perma.cc/4F59-MNPG].

147. U.S. CUSTOMS & BORDER PROT., *supra* note 18, at 1. For an example of an electronic border search that protected the safety of the U.S. citizens, see Waddell, *supra* note 17 ("[A] Vermont man . . . was arrested in February for allegedly having sex with a 13-year-old girl. Border agents stopped the pair as they tried to enter the U.S. from Canada and inspected the girl's phone. There, they found texts suggesting a sexual relationship with the 25-year-old man.").

148. U.S. CUSTOMS & BORDER PROT., *supra* note 17.

149. Chris Megerian & Brian Bennett, *U.S. Dramatically Increased Searches of Electronic Devices at Airports in 2017, Alarming Privacy Advocates*, L.A. TIMES (Jan. 5, 2018, 3:20 PM), https://www.latimes.com/politics/la-na-airport-search-devices-20180105-story.html [https://perma.cc/3NB6-DPWG].

150. *Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel: Hearing Before the Subcomm. on the Constitution of the Comm. on the Judiciary*, 110th Cong. 13 (2008) (statement of Larry Cunningham, Assistant Dist. Att'y, Bronx Cty.), https://www.govinfo.gov/content/pkg/CHRG-110shrg45091/pdf/CHRG-110shrg45091.pdf [https://perma.cc/ML66-TMVU].

151. FED. BUREAU OF INVESTIGATION, CYBER CRIME, https://www.fbi.gov/investigate/cyber [https://perma.cc/P92T-99AX].

152. *See, e.g.*, United States v. Cotterman, 709 F.3d 952, 956–57 (9th Cir. 2013) (appealing multiple convictions related to child pornography found on the defendant's computer when he was crossing the U.S.-Mexico border).

some criminals evading detection—which, in turn, diminishes the safety and security of the nation—seems to be an incontrovertibly well-founded concern.[153]

2. Individual Privacy Concerns

On the other hand, because cell phones and computers contain far more sensitive information—as well as a far larger amount of information—than can be held in luggage, privacy advocates are concerned about what border searches without any individualized suspicion would mean for the individual privacy rights of travelers.[154] The anxiety surrounding this shrinking of privacy rights seems justified by the fact that searches of electronic devices on the border have increased nearly fifty percent in the 2017 fiscal year.[155] Of the searches performed, the Department of Homeland Security's Office of the Inspector General found that many of these searches "were conducted improperly, without adequate supervision or preexisting policies."[156] While privacy proponents acknowledge that CBP's 2018 guidelines,[157] which require "reasonable suspicion" for "advanced" searches, are an "improvement," most argue that forensic searches are still too invasive.[158] The 2018 guidelines still do not require that CBP agents possess any individualized suspicion for "manual" or "forensic" searches of electronic devices when the search implicates a "national security concern"—even though most border searches could seemingly fall under this broad exception.[159]

---

153. *See* Alasaad v. Nielsen, No. 17-CV-11730-DJC, 2019 WL 5899371, at *8–*9 (D. Mass. Nov. 12, 2019).

154. Nixon, *supra* note 40.

155. Emily Birnbaum, *Border Entry Searches of Electronic Devices Up Nearly 50 Percent Last Year: Report*, THE HILL (Dec. 10, 2018, 5:22 PM), https://thehill.com/policy/technology/420654-border-entry-searches-of-electronic-devices-up-nearly-50-last-year-report [https://perma.cc/NM2Q-6U3V].

156. *Id.*; *see also* OFFICE OF INSPECTOR GEN., *supra* note 21.

157. U.S. CUSTOMS & BORDER PROT., *supra* note 17.

158. Miroff, *supra* note 18.

159. Esha Bhandari, *The Government's New Policy on Device Searches at the Border: What You Need To Know*, AM. C.L. UNION (Jan. 9, 2018, 12:45 PM), https://www.aclu.org/blog/privacy-technology/privacy-borders-and-checkpoints/governments-new-policy-device-searches [https://perma.cc/R34Y-7N78] (noting that "national security" is never clearly defined in the guidelines).

As technology continues to integrate into every part of everyday life,[160] privacy proponents are also concerned about the immense privacy risks that travelers may experience simply by passing through U.S. Customs.[161] Privacy proponents believe that a U.S. citizen crossing the U.S. border should, at least, have "the same rights as a person arrested under suspicion of a crime."[162] Specifically, social media accounts—which may be accessed during a "manual" search that requires no individualized suspicion of wrongdoing—can serve as "gateways into an enormous amount of [users'] online expression and associations, which can reflect highly sensitive information about that person's opinions, beliefs, identity and community."[163]

While CBP does not release information about the ethnicity or race of the detained travelers, there is an explicit concern among privacy advocates that racial profiling is and will continue to be a large factor in determining which travelers to detain.[164] A particular concern is that maintaining a low standard of suspicion for electronic device searches on the border will negatively affect Arab and Muslim communities the most.[165] Additionally, specific occupations—such as journalists, lawyers, and volunteers—have seen increasing incidents of questioning and searching of electronic devices on the border.[166]

---

160. For example, internet-connected refrigerators, Amazon Echo devices, and other "smart" products have already become normalized and popularized in modern society. Tara Marsh, *Home Evolution: The Rise of the Smart Home*, THE BULLETIN (Jan. 28, 2019, 3:24 PM), http://www.bendhomes.com/home-evolution-the-rise-of-the-smart-home/ [https://perma.cc/JVW8-Q9CA]; *see also* Viktoria Modesta, Neil Harbisson & Amal Graafstra, *How Technology Is Changing What It Means to be Human*, CNN (Sept. 13, 2018), https://www.cnn.com/style/article/designing-bodies-future/index.html [https://perma.cc/H37D-HY52] (discussing stories of three people who have integrated technology into their bodies).

161. Olivia Solon, *US Border Agents Are Doing 'Digital Strip Searches.' Here's How To Protect Yourself*, THE GUARDIAN (Mar. 31, 2017, 6:00 AM), https://www.theguardian.com/us-news/2017/mar/31/us-border-phone-computer-searches-how-to-protect [https://perma.cc/NXA7-VBE5].

162. Megerian & Bennett, *supra* note 149.

163. Tony Romm, *U.S. Government Begins Asking Foreign Travelers About Social Media*, POLITICO (Dec. 22, 2016, 5:23 PM), https://www.politico.com/story/2016/12/foreign-travelers-social-media-232930 [https://perma.cc/QQ53-SBPU].

164. Solon, *supra* note 161 ("All it's doing is greatly exacerbating the racial profiling problem at the border." (internal quotation marks omitted) (quoting Christina Sinha, staff attorney at the Asian Law Caucus)).

165. Romm, *supra* note 163.

166. Max Rivlin-Nadler, *Journalists, Lawyers, Volunteers Face Increased Scrutiny by Border Agents*, NPR (Feb. 15, 2019, 2:44 PM), https://www.npr.org/2019/02/15/695164916/journalists-lawyers-volunteers-face-increased-scrutiny-by-border-agents [https://perma.cc/G9LX-LJBW]; *see also Nothing to Declare: Why U.S. Border Agency's Vast Stop and Search Powers Undermine Press Freedom*, COMMITTEE TO PROTECT JOURNALISTS (Oct. 22, 2018), https://cpj.org/reports/2018/10/nothing-to-declare-us-border-search-phone-press-freedom-cbp.php [https://perma.cc/4QEZ-69DF].

Due to the prevalence of both technology and international travel in modern society, the question becomes whether it is fair that U.S. citizens' constitutional rights are being greatly diminished simply by being active participants in society. In this sense, it appears that the argument that the border search exception is stretching the limits of the Fourth Amendment too far is justifiable: "The idea that [U.S. citizens] can be searched just by entering or leaving the country we are citizens of . . . goes against the very thing that the 4th Amendment was designed to protect against, which is arbitrary dragnet surveillance."[167]

E. Possible Solutions: A Summary of Various Fourth Amendment Requirements

Noting the jurisprudential trend and strong policy arguments against the specific needs and desires of U.S. citizens and CBP, the Supreme Court inevitably will face pressure to create a bright-line rule in a murky area that will have broad implications on the lives of all Americans. While the plain text of the Fourth Amendment seems to require obtaining a warrant based on probable cause for all searches, the Supreme Court has carved out specific exceptions for when a search or seizure will be deemed reasonable without a warrant.[168] As the Court places more emphasis on the "reasonableness" clause of the Fourth Amendment, the roles of the warrant and probable cause provisions seem to be playing a role of diminishing importance.[169] Throughout Fourth Amendment jurisprudence, when determining whether a search or seizure is reasonable, the Court has generally found different situations fall under one of four possible requirements.

---

167. Megerian & Bennett, *supra* note 149.

168. The exigency exceptions to the warrant requirement include, but are not limited to, the following: Brigham City, Utah v. Stuart, 547 U.S. 398, 400 (2006) (the "emergency aid" exception); Arizona v. Hicks, 480 U.S. 321, 321 (1987) ("plain view" doctrine); United States v. Santana, 427 U.S. 38, 42–43 (1976) ("hot pursuit" of a fleeing suspect); Schneckloth v. Bustamonte, 412 U.S. 218, 248 (1973) (consent by the party).

169. Scott E. Sundby, *A Return to Fourth Amendment Basics: Undoing the Mischief of* Camara *and* Terry, 72 MINN. L. REV. 383, 385 (1988) (arguing that while the scope of the Fourth Amendment extends to government activities, the role of probable cause has diminished and thereby set the stage for the expansion of a "reasonableness balancing test without proper justification or limits").

1. Warrant Based on Probable Cause

A warrant based on probable cause is the default requirement for all searches and seizures.[170] This is because a search or seizure, absent probable cause, is presumptively unreasonable.[171] This is rooted in the language of the Fourth Amendment, which states that "no Warrants shall issue, but upon probable cause."[172] While probable cause is traditionally understood as the most stringent level of suspicion required under the Fourth Amendment, courts have debated over whether there may be an even stricter requirement for when the government intrudes upon a "significantly heightened privacy interest."[173]

A requirement of probable cause for forensic searches of electronic devices at the border does not sufficiently recognize the time constraints implicated at the border. For example, in order to obtain a search warrant at the border, a CBP agent would have to stop a traveler from continuing on in his journey, through either relying on consent, "reasonable suspicion," or another exception.[174] Then, the CBP agent would have to submit, with particularity,[175] a sworn statement or an affirmation stating that there is probable cause to believe a search of the traveler's electronic device is justified, along with the warrant itself.[176] Finally, the CBP agent would have to present his case to a neutral and detached judge, who then must decide whether to grant or deny his request.[177] If the judge granted the warrant, only then could the CBP agent perform a forensic search of the electronic device. As of this Comment's submission, no circuit court has advocated that a warrant based on probable cause should be required for any level of electronic search on the border.

---

170. *See* Kentucky v. King, 563 U.S. 452, 452 (2011).

171. Payton v. New York, 445 U.S. 573, 586 (1980).

172. U.S. CONST. amend. IV.

173. *See* Winston v. Lee, 470 U.S. 753, 767 (1985). In *Winston*, the Supreme Court held that the surgical removal of a bullet constitutes an unreasonable search under the Fourth Amendment. *Id*. at 759. The Court reasoned that while the public interest in obtaining evidence relevant to a criminal proceeding sometimes outweighs an individual's expectations of privacy under the Fourth Amendment, a severe intrusion—here, a surgery to remove a bullet—may be deemed unreasonable regardless of the probability of obtaining evidence. *Id*.; *see generally* Blake A. Bailey, Elaine M. Martin & Jeffery M. Thompson, *Criminal Law*—Lee v. Winston*: Court-Ordered Surgery and the Fourth Amendment—A New Analysis of Reasonableness?*, 60 NOTRE DAME L. REV. 149 (1984) (summarizing Supreme Court cases involving invasive intrusions).

174. United States v. Drayton, 536 U.S. 194, 194 (2002); *see infra* Part II.E.2.

175. Maryland v. Garrison, 480 U.S. 79, 83 (1987).

176. Illinois v. Gates, 462 U.S. 213, 238–39 (1983).

177. Coolidge v. New Hampshire, 403 U.S. 443, 443 (1971).

2. No Warrant but Based on an Exigency Exception

Under exigent circumstances, probable cause can justify a warrantless search or seizure.[178] Exigent circumstances permit law enforcement agents to conduct a search or seizure that would ordinarily violate the Fourth Amendment.[179] This exception is meant to encompass situations when it would be impractical to require an agent to obtain a warrant, such as when emergency aid may be required, when agents are in hot pursuit of a fleeing suspect, or when the imminent destruction of evidence may be prevented.[180]

While at first glance relying on an exigency exception, such as the imminent destruction of evidence, may seem to be a reasonable option, the necessity of probable cause would place too much of a hinderance on CBP agents and travelers alike. Probable cause is a totality of the circumstances test that asks whether a reasonably prudent person would believe that the search would reveal contraband or evidence of a crime.[181] Due to the extraordinary amount of data and ongoing nature of new data being created on electronic devices, an electronic device could potentially always reveal evidence of some type of crime; thus, this would not sufficiently address individual privacy concerns. Additionally, because of the multitude of persons crossing the U.S. border daily, it may be difficult for CBP agents to prove that they actually possessed probable cause for a forensic search of a specific electronic device; thus, this would not sufficiently protect national security. As of this Comment's submission, no circuit court has advocated that a warrantless search based on probable cause should be required for any level of electronic search on the border.

3. No Warrant but with "Reasonable Suspicion"

In certain situations, "reasonable suspicion" can justify a warrantless search or seizure.[182] "Reasonable suspicion" is a "fluid concept" that is less than probable cause but more than an "inchoate and unparticularized suspicion or 'hunch.'"[183] The Fourth Amendment permits brief investigative

178. Kentucky v. King, 563 U.S. 452, 452 (2011).

179. *Id*.

180. *Id*. at 460; *see supra* note 168.

181. Florida v. Harris, 568 U.S. 237, 238–39 (2013).

182. *See generally* Theodore P. Metzler et al., *Warrantless Searches and Seizures*, 89 GEO. L.J. 1084 (2001).

183. Terry v. Ohio, 392 U.S. 1, 27 (1968); Aliza Hochman Bloom, *When Too Many People Can Be Stopped: The Erosion of Reasonable Suspicion Required for a* Terry *Stop*, 9 ALA. C.R. & C.L. L. REV. 257, 260 (2018).

stops—also known as "stop and frisk"[184]—when a law enforcement agent observes conduct that reasonably leads him or her to conclude that crime is afoot and that specific individuals are involved in it.[185] This requirement gives agents broad discretion in determining which subjects to detain and search.[186] After a search has occurred, a court must complete a two-step inquiry to uphold its constitutionality: first, the court must determine whether the stop was justified at its inception; and second, the court must determine whether the stop was reasonably related in scope to the circumstances.[187]

The way that this approach works at the border is simply that a CBP agent would need to have "reasonable suspicion" that a specific electronic device may reveal evidence of criminal activity before he or she performs a forensic search of the traveler's electronic device. A CBP agent must then subsequently articulate this specific suspicion to a judge. As of this Comment's submission, both the Fourth and Ninth Circuits have advocated that "reasonable suspicion" should be required for forensic searches of electronic devices on the border.[188]

4. "No Suspicion"

In a few designated situations, law enforcement agents satisfy the reasonableness requirement with "no suspicion" at all. For example, law enforcement agents may stop travelers at fixed checkpoints near the border without individual suspicion even if the stop is largely based on ethnicity.[189] Additionally, law enforcement agents may stop and board ships on inland waters with "ready access to the sea" without any suspicion of wrongdoing.[190] The Supreme Court has also upheld the use of sobriety checkpoints generally without requiring individualized suspicion.[191]

This exception to the need for any "reasonable suspicion" is premised on a balancing of interests, namely: "[W]here the Fourth Amendment intrusion serves special governmental needs, beyond the normal need for law enforcement, it is necessary to balance the individual's privacy expectations

184. WILLIAM E. RINGEL, SEARCHES AND SEIZURES, ARRESTS AND CONFESSIONS §13:1 (Justin D. Franklin & Steven C. Bell eds., 2018).

185. *Terry*, 392 U.S. at 30.

186. RINGEL, *supra* note 184.

187. *Terry*, 392 U.S. at 19–21.

188. *See supra* Part II.C.1.

189. United States v. Martinez-Fuerte, 428 U.S. 543, 561–63 (1976) (concluding that the Fourth Amendment "imposes no irreducible requirement" for requiring some quantum of individualized suspicion as a prerequisite to a constitutional search or seizure).

190. United States v. Villamonte-Marquez, 462 U.S. 579, 579–80, 588 (1983).

191. Mich. Dept. of State Police v. Sitz, 496 U.S. 444, 450–51 (1990).

against the Government's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in a particular context."[192] The implementation of this approach on the border simply means that a CBP agent could seize a traveler's electronic device and conduct a manual or forensic search of it at any time for absolutely any reason. As of this Comment's submission, the Eleventh Circuit is the only circuit court to have advocated that "no suspicion" is required for any type of electronic search on the border.[193]

III. ANALYSIS

As the preceding case law emphasizes, technology is placing a strain on traditional Fourth Amendment jurisprudence. This is particularly true when deciding which level of suspicion should be required for forensic searches of electronic devices on the U.S. border. As discussed previously, requiring a warrant based on probable cause or relying on an exigency exception are not viable options, and no court has supported either of those requirements in this context. The harder question is the decision on whether "reasonable suspicion" or "no suspicion" better addresses the clash between technology and national security on the border.

Due to the growing prominence of this issue in state and federal courts, the Supreme Court should correct the current inconsistencies among the circuit courts. Following a similar analytical approach taken by the Court in previous circuit split decisions, the Court should factor the general trend of the lower courts' holdings into its decision. This would support a requirement of "reasonable suspicion" for forensic searches of electronic devices on the border.[194] However, because of the unique characteristics of the border—the high traffic of persons and belongings[195] and the need to act quickly to protect the nation from "dangerous people and material"[196]—the Court has repeatedly held that a significantly diminished expectation of privacy is appropriate. This would support a requirement of "no suspicion" for forensic

192. Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 665–66 (1989).

193. *See supra* Part II.C.2.

194. *See, e.g.*, Payton v. New York, 445 U.S. 573, 574–75, 587–89 (1980). While it is unknown exactly how much weight the circuit court trend factored into the Court's final holding, the five pages on which the Court incorporated the circuit jurisprudential trend into its analysis indicates that it was at least somewhat prominent. *Id*.

195. U.S. CUSTOMS & BORDER PROT., SNAPSHOT: A SUMMARY OF CBP FACTS AND FIGURES (2019), https://www.cbp.gov/sites/default/files/assets/documents/2019-Mar/CBP-Snapshot-03072019.pdf [https://perma.cc/9C8K-U5S8] (showing that on a typical day, CBP processes 1,133,914 passengers and pedestrians).

196. *Id*.

searches of electronic devices on the border. For these reasons, and because the government's interest in preventing the entry of unwanted persons and effects is at its zenith at the U.S. border, the most logical requirements for the Supreme Court to consider for forensic searches at the border should be either "reasonable suspicion" or "no suspicion"—mirroring the circuit split.

For three reasons, the Court should resolve this issue following the reasoning of the Ninth and Fourth Circuits that required individualized "reasonable suspicion" for forensic searches of electronic devices at the border. First, while *Riley v. California* and *Carpenter v. United States* were relatively narrow holdings, the reasoning behind these decisions clearly shows that digital property requires special treatment under the Fourth Amendment. Second, the Fourth Amendment balancing test clearly supports requiring "reasonable suspicion" for more intrusive searches, including forensic searches, due to the heightened privacy interests at stake. Third, if the "reasonable suspicion" standard was adopted, CBP could still perform quick searches of electronic devices on the border with "no suspicion."

First, the Court should decide that "reasonable suspicion" is required for forensic searches of electronic devices on the border following the reasoning in *Riley* and *Carpenter*, which shows that the Fourth Amendment treats technology differently. While *Riley* and *Carpenter* are narrow holdings particularly applicable in certain contexts when Fourth Amendment protections usually do not attach—*Riley* pertains to the search-incident-to-arrest doctrine and *Carpenter* pertains adjacently to the third-party doctrine—the Court's interpretation of the scope of the Fourth Amendment in these cases has a broader reach. In both *Riley* and *Carpenter*, the Court held that although these situations generally do not require any suspicion for a search to be deemed reasonable, the insertion of technology sometimes increases the level of suspicion constitutionally required. In both cases, the Court added protections to electronic devices by enhancing the level of suspicion required from "no suspicion" at all to the Fourth Amendment's most stringent requirement, a warrant based on probable cause. Since the Fourth Amendment protects both property and certain privacy interests, the insertion of technology, which greatly increases privacy concerns, necessitates greater Fourth Amendment protections.[197]

As explained in this Comment, the border is also a unique context where the Fourth Amendment's full protections traditionally do not attach.

197. But see *Criminal Procedure—Forensic Searches of Digital Information at the Border—Eleventh Circuit Holds That Border Searches of Property Require No Suspicion—*United States v. Touset*, 890 F.3d 1227 (11th Cir. 2018)*, 132 HARV. L. REV. 1112, 1117–19 (2019), for an argument that *Touset* was correctly decided and "no suspicion" is the correct requirement for forensic searches at the border.

However, as shown in *Riley* and *Carpenter*, because the technological component of electronic searches significantly impacts privacy interests, these types of searches warrant a special Fourth Amendment evaluation. Because of the similarities between the decisions in *Riley* and *Carpenter* and forensic searches of electronic devices at the border, the Court should follow a similar analysis when deciding on this issue.

In *Riley* and *Carpenter*, the insertion of technology pushed the level of suspicion required to the Fourth Amendment's most stringent requirement, a warrant based on probable cause. However, it is important to note that in both *Riley* and *Carpenter* the police presumably had more time to apply for a warrant. This longer time frame cannot be as easily presumed to be an option for government agents trying to react quickly to protect the nation on the border. Thus, while general Fourth Amendment principles and the jurisprudence surrounding the addition of technology would seem to point to requiring a warrant based on probable cause in cases that severely implicate an individual's privacy rights, the particularities of the border must inevitably lower this requirement. Since the touchstone of the Fourth Amendment remains reasonableness, it may be unreasonable to require CBP to obtain a warrant prior to an electronic search—as is required for government agents in *Riley* and *Carpenter*—due to the tighter time constraints and the need for national security protections. However, it does seem reasonable to require that CBP, at least, possess the relatively low standard of "reasonable suspicion" prior to conducting a forensic search due to the immense individual privacy concerns at stake.[198]

Second, when drafting the Fourth Amendment, the Framers certainly could not have contemplated the possibility, let alone the omnipresence, of a personal handheld Library of Congress. Absent more specific guidance from the founding era, the Court has evaluated reasonableness by assessing the intrusion on an individual's privacy interests against the promotion of legitimate governmental interests. On the subject of the border searches, the Court has previously only required "reasonable suspicion" for certain "highly intrusive searches" that implicate the "dignity and privacy interests of the person being searched."[199] Some argue that this higher standard is specifically a concern for the dignity of the person or a complete destruction of property, not just privacy in general, and therefore should not extend to electronic devices. While there is merit to the argument that invasive body searches are different from invasive electronic device searches, the *Riley* and *Carpenter*

198. This Goldilocks Principle reasoning has previously been supported by the Supreme Court. *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 10–13, 27 (1968).

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

decisions show that the Supreme Court and the Fourth Amendment do not limit themselves so easily to such a distinction.

The rapid advancement in technology must necessarily affect the traditional Fourth Amendment analysis. As the Supreme Court in *Carpenter* noted, because the government's capacity to encroach upon historically protected areas through technology has increased, the Court has generally sought to preserve the degree of privacy from governmental intrusion that existed when the Fourth Amendment was adopted. Because searches on the border are justifiable merely by occurring on the border and these searches will generally be related to the governmental interest of protecting national security, a lower standard of suspicion is reasonable. Nevertheless, due to the invasiveness of a forensic search and the prominence of electronic devices among travelers, a slightly heightened requirement of "reasonable suspicion" would be the correct balance.[200] Thus, while requiring a lower standard of suspicion promotes the government's interest in national security, because forensic searches can reveal basically everything about an individual's identity, the vast intrusion on individual privacy interests should mandate CBP have, at least, individualized "reasonable suspicion" prior to a forensic search.

Third, under this requirement, quick searches[201] of electronic devices on the border are still allowed without any individualized suspicion requirement. This means that even if the higher standard were adopted for forensic searches, CBP would still be able to superficially search electronic devices based solely on a generalized "hunch" or random selection. Adding the additional protections to forensic searches would thus only prohibit overly invasive searches where CBP is specifically targeting individuals for reasons not necessarily related to national security. Examples of this type of targeting would be if CBP used factors such as an individual's race, religion, occupation, or political party when deciding whose electronic devices to search. As these targeted searches do not advance national security, "reasonable suspicion" for forensic searches on the border correctly balances national security and individual privacy needs.

Due to the strength of the opposing policy interests, a decision on this matter would likely cause intense scrutiny and criticism from the "losing" side. However, because of the large quantity of travelers crossing the U.S.

---

200. *See infra* Part II.E.3. However, part two of the *Terry* test states the scope of the search must be reasonably related to the circumstances. Since electronic devices contain so much information that may not be reasonably related to a border search, this is where the circumstances could arguably stretch the *Terry* doctrine too much and would warrant a higher requirement.

201. Referred to generally as either "manual" or "basic" searches. *See supra* note 19–21 and accompanying text.

border daily and the pervasiveness of electronic devices among those travelers, until the Supreme Court decides this issue, the inconsistencies between circuits will inevitably hinder both individual privacy and national security. While the CBP's 2018 directive's adoption of a "reasonable suspicion" standard adds some protections to this area, the directive does not mean "reasonable suspicion" is constitutionally mandated. Additionally, the directive creates large exceptions to many of the privacy safeguards it seems to promote.[202] Because the "reasonable suspicion" standard most equitably balances the privacy needs of Americans against the needs of the U.S. government in maintaining national security, the Court should find the Fourth Amendment requires "reasonable suspicion" for forensic searches of electronic devices at the border.

IV. CONCLUSION

The Supreme Court should hear an appropriate case to address this issue. While seemingly a narrow issue, the vast reach of both electronic devices and international travel means that this issue—whether or not an individual is selected to be searched—necessarily effects the entire nation. Until the circuit split is resolved, the constitutional rights of all Americans hang in the balance. Weighing the importance of providing CBP with the necessary tools to protect national security against the gravity of the individual privacy invasion, the Court should deem forensic searches of electronic devices at the border without "reasonable suspicion" as unreasonable under the Fourth Amendment. With the *Riley v. California* and *Carpenter v. United States* decisions, the Court has repeatedly held that the Fourth Amendment compels specific protections when technology and electronic devices are involved. Following this reasoning, the Court should decide the circuit split in favor of the Fourth and Ninth Circuits and conclude that the Fourth Amendment requires government agents to have individualized "reasonable suspicion" prior to conducting forensic searches of electronic devices at the border. If "reasonable suspicion" were the requirement, then maybe Sidd's cell phone would not have been confiscated at the border, and he would have just been mindlessly scrolling through Facebook like the rest of us.

202. *See supra* note 22 and accompanying text.