THE HIDDEN CRISIS AT THE BORDER: THE GOVERNMENT'S CARTE BLANCHE ACCESS TO TRAVELERS' ELECTRONIC DEVICES AND THE NEED TO REIMPLEMENT REASONABLENESS

Sean Mullen*

I. INTRODUCTION

Policy debates over the southern border of the United States have come to a boiling point and created high tension amongst the populace. Political rhetoric is freely dispersed and unwavering partisan ideology has become far more prevalent than compromise or understanding. All the while, technological advances and our dependence on electronic devices have encouraged the government to usurp constitutional protections. What is more, courts have supplied the government with various outmoded doctrines to do so. The border search exception to the Fourth Amendment[1] warrant requirement has served as a trump card for the government to perform limitless searches of items crossing the border.[2] However, requiring a warrant for the search of an electronic device—as has been found to be appropriate in every other context—complies with the dual intent of the Founders to protect the integrity of the country's borders and simultaneously prevent a police state where

 Juris Doctor, magna cum laude, Stetson University College of Law, 2020; B.A. in Political Science, summa cum laude, University of South Florida, 2017. I would like to thank Professor Virelli, Former Notes & Comments Editor Eric Lyerly, Former Executive Editor Brian Remler, Former Editor in Chief Kelly Jackson, and Former Articles and Symposia Editor Megan Powell for their assistance throughout the writing and editing of this Article. In addition, I would like to thank all the hard-working editors and associates from Stetson Law Review that worked on editing this Article.

1. The Fourth Amendment guarantees:

> 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.

U.S. CONST. amend. IV.

2. *Warrantless Searches and Seizures*, 39 GEO. L.J. ANN. REV. CRIM. PROC. 43, 121 (2010).

the government can arbitrarily and unreasonably intrude on the privacy of citizens.

Each year, millions of Americans travel abroad and are at risk of government confiscation of their electronic devices and the information on those devices.[3] Although individuals' expectation of privacy is fundamentally lower at the border, the qualitative and quantitative differences in the data available on electronic devices implicate the need for the full force of the Fourth Amendment. The Supreme Court has articulated that "[w]ith all [that electronic devices and cell phones] contain and all they may reveal, they hold for many Americans 'the privacies of life.'"[4]

This Article discusses the need to apply the warrant requirement to forensic searches of electronic devices when they are carried across customs entry and exit points, as the Supreme Court has recently mandated with searches incident to a valid arrest.[5] Since cell phones are qualitatively and quantitatively different from other objects subject to search, and the contents that may be gathered from them do not comport with the original intent of the border search exception, the Fourth Amendment requires border agents to secure a warrant before confiscating a cell phone and investigating its content. This Article argues that the warrant requirement is the most constitutionally appropriate procedure for conducting searches of cell phones and other electronic devices—a category never considered before by the Supreme Court as it relates to border searches—because these searches are inherently highly intrusive.

This Article does not focus exclusively on the southern border. With the extensive media coverage and focus on the southern border by politicians from all political parties, it is easy to immediately associate any "border" topic with the southern border and forget all others. Instead, the threat of government intrusion is just as real and significant at an international airport in Tampa, Chicago, Charlotte, or any other location where citizens travel to or from *any* foreign destination. This issue should be viewed in light of the threat of government intrusion for all Americans. Furthermore, the scope of this Article is focused on the government's practice of hacking into the electronic devices of

3. Nat'l Travel and Tourism Office, *U.S. Citizen Travel to International Regions 2018*, U.S. DEP'T OF COM. (Feb. 2019), https://travel.trade.gov/view/m-2018-O-001/index.html. In 2018 alone, over 9.3 million American citizens traveled internationally. *Id.* This represented an increase of 6.3 percent from 2017. *Id.*

4. Riley v. California, 573 U.S. 373, 403 (2014) (citing Boyd v. United States, 116 U.S. 616, 630 (1886)).

5. *Id.* at 403.

unsuspecting travelers with machines designed to pull data from phones. This is starkly different from law enforcement officials doing a mere physical safety inspection of electronic devices on the scene—which officers may still conduct to ensure their safety.[6]

Part I of this Article addresses the historical context and purpose of the border search exception to the warrant requirement; Part II addresses Department of Homeland Security (DHS) policies and practices regarding searches of electronic devices at the border; Part III analyzes the decision in *Riley v. California*[7] and the post-*Riley* fallout from the holding; and Part IV concludes this Article by explaining why the balancing test between the rights of citizens and government interests favors privacy rights when it comes to forensic searches of electronic devices, and urging Congress and the Supreme Court to apply the same warrant requirement in *Riley* to electronic devices at the border.

II. HISTORICAL CONTEXT AND PURPOSE OF THE BORDER SEARCH EXCEPTION

This Part provides a historical overview of Congress' heightened interest in keeping contraband from passing through the entry and exit points of the country and how the border search exception to the warrant requirement interplays with that goal. In addition, this Part will contextualize what types of searches and items were contemplated under the ambit of the border search exception.

A. The Underpinnings of the Heightened Government Interest

The government's interests have been recognized to be at their "zenith"[8] at points of entry and exit from the country,[9] and the notion that an individual's privacy expectations are lessened at the border is

6. *Id.* at 374.

7. *Riley* provided the groundwork from which all future challenges to the constitutionality of warrantless searches of electronic devices was laid. *See*, *e.g.*, State v. Lietzau, 463 P.3d 200, 200–03 (S. Ct. Az. 2020) (holding that, in light of *Riley*, cell phones are not simply property and thus are not protected by the border search exemption from the Fourth Amendment warrant requirement). The importance of the decision as it effects privacy rights should not be understated.

8. The United States has inherent sovereign authority to protect the paramount interest of securing its territorial integrity. United States v. Flores-Montano, 541 U.S. 149, 152–53 (2004). Amongst the most important roles of any government is protecting the safety and well-being of its citizens. *See The Purposes of Government*, USHISTORY.ORG, http://www.ushistory.org/gov/1a.asp (last visited Sept. 23, 2020). It is axiomatic that the task of keeping contraband out of the country is made exponentially more difficult once contraband has made it to the interior.

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

well-established by caselaw.[10] The Fourth Amendment establishes both: (1) the right to be free from unreasonable government searches, and (2) warrant requirements that must be satisfied before such searches can occur.[11] In 1790, the same Congress that proposed the Fourth Amendment also enacted the first statute to extensively address searches at the border.[12]

The First Congress required officers to have "reason to suspect" the concealment of "goods, wares or merchandise, subject to duty" to "enter any ship or vessel . . . to search for, seize, and secure any such goods, wares or merchandise."[13] Indeed, even from the beginning, a textual reading of the statute intimates that Congress intended some level of suspicion be present for a search to be lawful. This reflects the government's heightened interest in preventing unwanted persons and tangible contraband from entering the country's borders, but it is not an unfettered right for government intrusion.[14]

The border search exception also extends far beyond traditional ports of entry and exit. The extended border search doctrine holds that government officials can conduct a warrantless search beyond the border only if three factors are together present: (1) there is "reasonable certainty" or a "high degree of probability" that there was a border crossing; (2) there is "reasonable certainty" that no change in the object of the search has occurred between the time of the border crossing and the search; and (3) there is "reasonable suspicion" of criminal activity.[15] Most forensic searches of electronic devices are conducted miles away from the initial border checkpoint where contact was first made.[16] Multiple circuits have slight differences on how far the exception is extended, but it is generally accepted that the exception is necessary so that law enforcement can practically and effectively accomplish its mission.[17]

---

10. United States v. Montoya De Hernandez, 473 U.S. 531, 537–38 (1985).

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

12. Act of Aug. 4. 1790, § 31, 1 STAT. 145. 164–65 (1790).

13. Act of July 31, 1789, ch. 5, § 24, 1 STAT. 29, 43 (the Congress which proposed the Bill of Rights to the state legislatures on September 25, 1789, had two months prior to that proposal enacted this first customs statute). Act of September 29, 1789, ch. 27, 1 Stat. 97, 97–98.

14. *See also Flores-Montano*, 541 U.S. at 152–53.

15. *Warrantless Searches and Seizures*, 39 GEO. L.J. ANN. REV. CRIM. PROC. 43, 121 (2010).

16. Benjamin J. Rankin, Note, *Restoring Privacy at the Border: Extending the Reasonable Suspicion Standard for Laptop Border Searches*, 43 COLUM. HUM. RTS. L. REV. 301, 320 (2011).

17. The Fifth Circuit recognizes a reasonable certainty standard for extended searches, defined as "more than probable cause, but less than proof beyond a reasonable doubt." United States v. Cardenas, 9 F.3d 1139, 1148 (5th Cir. 1993). The Ninth Circuit uses a totality of the circumstances test. United States v. Sahanaja, 430 F.3d 1049, 1054 (9th Cir. 2005); *see also* United States v. Oriakhi, 57 F.3d 1290, 1295–96 (4th Cir. 1995); United States v. Hyde, 37 F. 3d 116, 123 (3d Cir. 1994);

B. Routine and Nonroutine Searches: A Muddled Distinction with Different Implications

1. Routine Searches

There has long been a recognition that the ability to invoke Fourth Amendment protections is limited at the border.[18] The Supreme Court confirmed the importance of this legitimate interest and established a border search exception to the warrant requirement.[19] This exception loosens Fourth Amendment protections at the border and provides law enforcement officials greater latitude by removing the requirement of a

---

United States v. Haley, 743 F.2d 862, 864–65 (11th Cir. 1984); United States v. Ajlouny, 629 F.2d 830, 834 (2d Cir. 1980).

18. *See generally* Carroll v. United States, 267 U.S. 132, 153–54 (1925) (recognizing there is a distinction between searches at the border and those conducted within the interior). The *Carroll* Court stated:

> It would be intolerable and unreasonable if a prohibition agent were authorized to stop every automobile on the chance of finding liquor and thus subject all persons lawfully using the highways to the inconvenience and indignity of such a search. Travellers may be so stopped in crossing an international boundary because of national self protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in. But those lawfully within the country, entitled to use the public highways, have a right to free passage without interruption or search unless there is known to a competent official authorized to search, probable cause for believing that their vehicles are carrying contraband or illegal merchandise.

Id.; *see also* United States v. Thirty-Seven Photographs, 402 U.S. 363, 376 (1971).

> [O]bscene materials may be removed from the channels of commerce when discovered in the luggage of a returning foreign traveler even though intended solely for his private use. That the private user under Stanley may not be prosecuted for possession of obscenity in his home does not mean that he is entitled to import it from abroad free from the power of Congress to exclude noxious articles from commerce. *Stanley's* emphasis was on the freedom of thought and mind in the privacy of the home. But a port of entry is not a traveler's home. His right to be let alone neither prevents the search of his luggage nor the seizure of unprotected, but illegal, materials when his possession of them is discovered during such a search.

Id.

19. *See generally Carroll*, 267 U.S. at 153–54 (asserting that domestic, but not international, travelers may avoid warrantless searches).

warrant while conducting *routine*[20] searches.[21] Searches at the border are generally held to be reasonable "simply by virtue of the fact that they occur at the border."[22] Routine searches of entrants and their belongings at the border "are not subject to any requirement of reasonable suspicion, probable cause, or warrants."[23] Suspicionless routine searches of vehicles,[24] mail,[25] and persons[26] have all been upheld by the Supreme Court. Significantly, the border search exception is not limited to items entering the country, but also allows for the warrantless and suspicionless search of items leaving the country.[27]

2. Nonroutine Searches

Although *routine* searches at the border are exempt from the warrant requirement, the Supreme Court has consistently reasoned that *nonroutine* searches do require a particular level of suspicion.[28] A search crosses the threshold and becomes nonroutine if it is particularly offensive or physically destructive.[29] Accordingly, both *United States v. Montoya De Hernandez* and *United States v. Flores-Montano* held that the warrant exception is not unfettered and does not extend to searches beyond the scope of a routine customs search.[30]

In *Montoya De Hernandez*, customs officials detained the respondent after she arrived at Los Angeles Airport from Bogota,

20. There is not a clear definition or list from the Supreme Court on what a routine search is at the border. Society generally intuitively can assume that certain practices are routine from what has become expected through customs and practices widely known to the public. For example, most know that law enforcement officials at the border may do basic searches of vehicles at checkpoints. However, what we are left with to decide what is routine or not can be inferred from what has been found to be routine and nonroutine by the Court. *E.g.*, United States v. Montoya De Hernandez, 473 U.S. 531, 538 (1985) (finding that holding a suspect for sixteen hours before defendant passed balloons filled with cocaine from her alimentary canal was beyond the scope of a routine search); United States v. Flores-Montano, 541 U.S. 149, 155 (2004) (holding that the government taking possessory interest in a vehicle crossing the border and removing, disassembling, and reassembling the gas tank was within the scope of a routine search).

21. *Flores-Montano*, 541 U.S. at 152–53.

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

23. *Montoya De Hernandez*, 473 U.S. at 538.

24. *Carroll*, 267 U.S. at 154 (finding "[t]ravellers may be so stopped in crossing an international boundary because of national self protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in").

25. *Ramsey*, 431 U.S. at 620.

26. Almeida-Sanchez v. United States, 413 U.S. 266, 272 (1973).

27. *See, e.g.*, United States v. Odutayo, 406 F.3d 386, 391 (5th Cir. 2005) (joining the Second, Third, Fourth, Sixth, Eighth, and Ninth Circuits in extending the border search exception to outgoing travel).

28. *E.g.*, *Montoya De Hernandez*, 473 U.S. at 541.

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

30. *Flores-Montano*, 541 U.S. at 155–56; *Montoya De Hernandez*, 473 U.S. at 541.

Colombia.[31] Officials convicted her of various federal narcotics offenses after finding eighty-eight cocaine-filled balloons in her alimentary canal.[32] The Court elucidated that anything beyond a routine search at the border would require some level of reasonable suspicion, even if the Court did not specify what that particular level would be.[33]

In its decision, the Court held "that the 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 is smuggling contraband in her alimentary canal."[34] Because of the nonroutine nature of inspecting an alimentary canal, the Court required a "particularized and objective basis for suspecting the particular person" for the search and seizure to be appropriate.[35] The Court found the customs officials had such reasonable suspicion, and did not violate the respondent's rights by detaining her until they could confirm whether she had contraband inside her body.[36]

Montoya De Hernandez held that the search of the body was nonroutine and thus required reasonable suspicion.[37] The Court relied on past precedent to stop there. It noted, "Congress has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country."[38] Importantly, "the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is also struck much more favorably to the Government at the border."[39] Although this may be well-settled law for traditionally considered contraband, the storage capabilities of electronic devices yield far more intrusive searches and should tip the balance back to the Fourth Amendment's warrant requirement.[40]

Another Supreme Court decision helped to define a nonroutine search by providing an example of a routine search. In *United States v. Flores-Montano*, "[c]ustoms officials seized [thirty-seven] kilograms . . . of marijuana from respondent Manuel Flores-Montano's gas tank at the

31. United States v. Montoya De Hernandez, 473 U.S. 531, 532 (1985).
32. *Id.* at 532–33.
33. *Id.* at 541.
34. *Id.* (emphasis added).
35. *Id.* (quoting United States v. Cortez, 449 U.S. 411, 417 (1981)).
36. *Id.* at 544.
37. *Id.* at 541.
38. *Id.* at 537.
39. *Id.* at 540.
40. *Infra* pt. IV.

international border."[41] The government argued that the disassembly and reassembly of a gas tank to examine its contents was a routine search and therefore did not require reasonable suspicion.[42]

The United States Court of Appeals for the Ninth Circuit ruled in favor of Flores-Montano and held that "the Fourth Amendment forbade the fuel tank search absent reasonable suspicion."[43] The Supreme Court reversed the Ninth Circuit and held that "the Government's authority to conduct suspicionless inspections at the border includes the authority to remove, disassemble, and reassemble a vehicle's fuel tank."[44] However, the Court did caution that some searches of property may be "so destructive as to require a different result."[45] This final caveat may seem small, but in fact, it dispels the notion that *all* physical property may be rummaged through without regard to constitutional considerations.

Before the *Riley v. California*[46] decision in 2014, the Ninth Circuit, in *United States v. Cotterman*, applied the border search exception to electronic devices and held that forensic searches of computers at the border require some level of suspicion.[47] The *Cotterman* Court seized on the language of the Supreme Court in *Flores-Montano* in holding that an individual's privacy interest of an individual "at the border will on occasion demand 'some level of suspicion in the case of highly intrusive searches of the person.'"[48] Moreover, the Court distinguished electronic devices from other less sophisticated tangible items like in its decision in *Flores-Montano* by reasoning that the "private information individuals store on digital devices—their personal 'papers' in the words of the Constitution—stands in stark contrast to the generic and impersonal contents of a gas tank."[49]

41. 541 U.S. 149, 150 (2004).
42. *Id.* at 151.
43. *Id.* at 150.
44. *Id.* at 155.
45. *Id.* at 155–56; *see, e.g.*, United States v. Rivas, 157 F.3d 364, 367–68 (5th Cir. 1998) (holding that drilling into a metal trailer required reasonable suspicion because it was nonroutine); United States v. Robles, 45 F.3d 1, 5–6 (1st Cir. 1995) (holding that drilling into a metal cylinder was a nonroutine search that was justified by the government's reasonable suspicion).
46. 573 U.S. 373 (2014); *infra* pt. III.
47. 709 F.3d 952, 968 (9th Cir. 2013).
48. *Id.* at 963. Similarly, the court pointed to the Supreme Court's previous reasonings: "'[S]ome searches of property are so destructive,' 'particularly offensive,' or overly intrusive in the manner in which they are carried out as to require particularized suspicion." *Id.* (citing *Flores-Montano*, 541 U.S. at 152, 154 n.2, 155–56; United States v. Montoya De Hernandez, 473 U.S. 531, 541 (1985).
49. *Cotterman*, 709 F.3d at 964; *see also* United States v. Jones, 565 U.S. 400, 418 (2012) (Sotomayor, J., concurring) (intimating "doubt that people would accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year").

The Ninth Circuit noted that the reasonable suspicion requirement is not unmanageable for border control because it merely "requires that officers make a commonsense differentiation between a manual review of files on an electronic device and application of computer software to analyze a hard drive, and utilize the latter only when they possess a 'particularized and objective basis for suspecting the person stopped of criminal activity.'"[50] This precursor to *Riley* was the court reestablishing that it is not "anything goes" at the border, and an individual's dignity and privacy rights are not abandoned, but instead are "[b]alanced against the sovereign's interests."[51]

The Supreme Court has not explicitly distinguished a routine from a nonroutine border search; however, this has not stopped circuit courts from using various factors to designate a search as nonroutine.[52] Generally, the difference between a routine search and a nonroutine search has turned on the subjective level of intrusiveness involved in a particular circumstance.[53]

III. DHS POLICIES AND PRACTICES OF SEARCHING ELECTRONIC DEVICES

Perhaps seeing the writing on the wall,[54] the U.S. Customs and Border Protection Agency (CBP) published a directive in 2018 that lays out its policies for conducting searches of electronic devices at the

50. *Cotterman*, 709 F.3d at 967 (quoting United States v. Tiong, 224 F.3d 1136, 1140 (9th Cir. 2000)).

51. *Id.* at 960 (internal citations omitted).

52. *See* United States v. Braks, 842 F.2d 509, 512 (1st Cir. 1988). The First Circuit considered six factors when determining between a "routine" and "nonroutine" search:

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

Id.

53. *See Flores-Montano*, 541 U.S. at 152 (mentioning highly intrusive searches of a person that offend his or her dignity and privacy interests as searches that could be deemed nonroutine and require some level of suspicion).

54. *See infra* pt. III.

border.[55] The Directive covers "CBP Officer[s], Border Patrol Agent[s], Air and Marine Agent[s], Office of Professional Responsibility Agent[s], and other officials authorized by CBP to perform border searches."[56] Furthermore, it defines electronic devices as "[a]ny device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players."[57]

It is noteworthy that the Directive seems to premise any self-restricting policy decision on the idea that CBP has no responsibility to do so. The Directive provides a long history of caselaw (much of which has been or will be extensively covered in this Article) and statutes that apparently, in the CBP's view, grant the Agency unlimited ability to conduct searches at its discretion without any other constitutional checks.[58] Very graciously, the Directive proclaims:

> CBP's broad authority to conduct border searches is well-established, and courts have rejected a categorical exception to the border search doctrine for electronic devices. Nevertheless, as a policy matter, this Directive imposes certain requirements, above and beyond prevailing constitutional and legal requirements, to ensure that the authority for border search of electronic devices is exercised judiciously, responsibly, and consistent with the public trust.[59]

To the contrary, these "above and beyond" policies do not ensure that searches are exercised "judiciously, responsibly, and consistent with public trust."[60]

This Article argues wholeheartedly that those three pillars are essential to protecting a person's due process guarantees;[61] however, the current policies fall well short of any such benchmark and are unreasonable under the Fourth Amendment. The CBP's narrative is important because it maintains that none of its policies in the Directive are mandated by statute or constitutional authority.[62] Moreover, the CBP relies on its own interpretation of caselaw to conclude that border

55. U.S. Customs and Border Prot., CBP Directive No. 3340-049A, Border Search of Electronic Devices 1 (2018) [hereinafter Border Search of Electronic Devices].

56. *Id.* ¶ 2.2.

57. *Id.* ¶ 3.2.

58. *Id.* ¶ 4.

59. *Id.*

60. *Id.*; *see infra* pt. IV.

61. The Fifth Amendment, in part, provides that a person shall not be "deprived of life, liberty, or property, without due process of law." U.S. CONST. amend. V.

62. Border Search of Electronic Devices, *supra* note 55, ¶ 4.

searches of electronic devices are essentially exempt from any Fourth Amendment requirements[63]—the same "anything goes" mentality that the Ninth Circuit held to be false in *Cotterman*.[64]

In addition, notably missing from the Directive is any means for a traveler to object to a search of an electronic device other than going through the courts post-inspection. This makes the need for constitutional protections even more urgent.

A. Types of Searches

There are two types of searches covered by the Directive: basic and advanced searches.[65] According to the Directive, officers may not access information that is only stored on remote platforms.[66] Officers must ask the traveler to disable connectivity to any networks or do it themselves when appropriate.[67]

For passcode-protected or encrypted information, the Directive obligates travelers to provide the passcodes to the device and any software applications (apps) on it so that officials may conduct a full search.[68] Indeed, if the traveler refuses to provide a password, the CBP's policy grants officers the authority to detain the device and use forensic-analysis instruments and other technical assistance to break into the device for full inspection.[69] These onerous inspections become even more intimidating for travelers who might not wish to provide their passwords to CBP agents.[70]

---

63. *Id.*
64. United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013).
65. Border Search of Electronic Devices, *supra* note 55, ¶¶ 5.1.3–5.1.4.
66. *Id.* ¶ 5.1.2.
67. *Id.*
68. *Id.* ¶ 5.3.3.
69. *Id.* ¶ 5.3.4
70. *See* Soo Youn, *Apple Employee Detained by US Border Agents Over His iPhone and Laptop Speaks Out*, ABC NEWS (Apr. 5, 2019, 5:48 PM), https://abcnews.go.com/US/apple-employee-detained-us-border-agents-iphone-laptop/story?id=62177572. This article tells the story of an Apple employee who refused to consent to CBP search of his laptop and phone. Although the entire encounter is troubling, the following excerpts show the real danger to everyone's privacy concerns and the potential for further overreach by CBP agents:

> "They insisted on searching the contents of my cell phone and my laptop that were issued to me by Apple," Gal told ABC News. "Which put me in a difficult situation because I signed NDAs (non-disclosure agreements) for those devices. They are owned by Apple and they contain proprietary information from Apple."
>
> . . .
>
> "That seemed to aggravate these customs agents and they started getting very upset with me and they said they had the right to access my devices and I had to turn over my passport," Gal said. "I told them I wanted to talk to an attorney and my employer so I could understand my responsibilities with regard to this NDA."

1. Basic Searches

Basic searches are any physical or cursory search of electronic devices that are conducted without an officer connecting the phone to an external hacking machine.[71] These searches require no suspicion whatsoever, and officers may review and analyze any information they see on the phone.[72] Although no hacking device is used, officers can still comb through a phone's contents and have access to a person's most personal and private conversations and photos.[73] Inferences and false assertions can easily give the illusion of "reasonable suspicion" to perform an even more intrusive search. This is akin to allowing the government to walk through a person's house without permission and open drawers until they see something that gave them some semblance of suspicion.

2. Advanced Searches

Advanced searches are defined as "any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents."[74] The CBP Directive requires that officers have *reasonable suspicion and supervisory approval* to conduct these searches, revealing its awareness of the intrusive nature of such searches.[75]

The examples proffered by the CBP regarding what may give rise to reasonable suspicion for these types of searches are striking. Examples given were monitoring for potential circumstances relevant to national security "in combination with other articulable factors as appropriate, or the presence of an individual on a government-operated and government-vetted terrorist watch list."[76] These seem reasonable, but are also factors that would likely make a warrant easy to obtain. In

---

. . .

> "They told me at the border, even as a U.S. citizen, I don't have any rights to an attorney," Gal, who became a U.S. citizen three years ago, said. "I told them I wanted to speak to an attorney. Then they said they would keep my devices and I said I don't consent to it but I would comply."

Id.

71. Border Search of Electronic Devices, *supra* note 55, ¶¶ 5.1.3–5.1.4.
72. *Id.* ¶ 5.1.3.
73. *Id.* ¶ 5.1.2.
74. *Id.* ¶ 5.1.4.
75. *Id.*
76. *Id.*

practice, such extreme examples are not the type that CBP needs to meet the reasonable suspicion standard. Reasonable suspicion is a subjective test that only requires an officer "to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion."[77]

B. Detention of Devices

The Directive permits officers to confiscate devices for as long as they determine is reasonably necessary for them to extract and analyze the data.[78] Although there are guidelines as far as extension procedures, the length of time an electronic device may be seized is constructively indefinite;[79] there is only the requirement that a supervisor approve of the continued detention.[80] Under the low standard of reasonable suspicion, a person who is traveling overseas for vacation could have their phone seized for the duration of their trip. The Directive acknowledges CBP's power to perform such a seizure.[81] Remember, a "basic search" needs no suspicion whatsoever according to both the CBP and most courts. There are frightening consequences to these lenient search standards. Officials can merely cry "reasonable suspicion" after their initial search to invoke their power to confiscate and access a traveler's phone—a likely scenario that will result from the Directive.[82]

IV. RILEY AND POST-RILEY EFFECTS ON BORDER SEARCHES

Riley v. California breathed life into the concept of reasonableness regarding searches of personal electronic devices. In *Riley*, the Supreme Court held that police must have a valid warrant to search cell phones incident to a valid arrest.[83] Although the decision was made in context of a search incident to a valid arrest, the analysis the Court applied to electronic devices and the intrinsic privacy concerns attached to them is instructive across all search spectrums.

77. Terry v. Ohio, 392 U.S. 1, 21 (1968).
78. Border Search of Electronic Devices, *supra* note 55, ¶ 5.4.1.
79. *See id.*
80. *Id.* ¶ 5.4.1.1 (providing that the standard time for detention is no more than five days, but that after that time frame, the detention can be extended with supervisor or director approval in increments of seven days, with no mention of a hard deadline for return of the property).
81. *Id.*
82. *Id.* ¶ 5.1.4.
83. 573 U.S. 373, 403 (2014).

A. *Riley* and the Return to Reasonableness

Riley examined two cases with the common question of whether a warrantless search of a cell phone was reasonable under the incident to a valid arrest exception to the warrant requirement.[84] The Court acknowledged, as CBP also felt compelled to point out in the border context,[85] there has been a longstanding "right on the part of the Government, always recognized under English and American law, to search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime."[86] However, the Court recognized that cell phones were a category not yet considered and are vastly different from searches of any other physical items.[87] The Court openly acknowledged that it had previously rejected a case-by-case analysis in *United States v. Robinson*,[88] but the *Riley* Court explained that it was instead examining digital data as a "particular category of effects" altogether.[89]

The Court in *Riley* used a balancing test "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[90] The Court quickly concluded that cell phones are quantitatively and qualitatively different than other physical items that may be searched.[91]

From a quantitative standpoint, the Court distinguished cell phones because of their "immense storage capacity."[92] It noted that "[m]ost 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. . . ."[93] Moreover, even if they could, it would require a trunk of some sort that would likely require a warrant.[94]

---

84. *Id.* at 378.
85. Border Search of Electronic Devices, *supra* note 55, ¶ 4.
86. *Riley*, 573 U.S. at 382. (quoting Weeks v. United States, 232 U.S. 383, 392 (1914)).
87. *Id.* at 385.
88. In *Robinson*, an officer examined a crumpled cigarette package in the defendant's pocket after an arrest for a traffic violation and the Defendant challenged the search was unreasonable because the crumpled packaged could be mistaken for a weapon. United States v. Robinson, 414 U.S. 218, 223 (1973). The Court concluded "A custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification." *Id.* at 235.
89. *Riley*, 573 U.S. at 386.
90. *Id.* at 385 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).
91. *Id.* at 393.
92. *Id.*
93. *Id.* at 393–94.
94. *Id.* at 394.

Qualitatively, cell phones may reveal "detailed information about all aspects of a person's life."[95] This includes extensive information like browsing history, geolocation data, photographs, purchasing history, and countless apps that provide users with many different tools for managing their lives.[96] The amount of information that could be pieced together by examining the data stored in a cell phone could not be acquired through searching a wallet, suitcase, or other tangible item.[97]

In defense of its position, the government argued that data stored on an electronic device is "materially indistinguishable" from similar searches of other physical items.[98] In an immediate repudiation of the government's position, the Supreme Court found there was no way digital data could be lumped together with searches of other physical items.[99]

After weighing the government's minimal interests in these searches against the unique privacy interests at stake, the Court held "that officers must generally secure a warrant before conducting such a search."[100] Chief Justice Roberts, in a nearly unanimous decision, wrote the "answer to the question of what police must do before searching a cell phone seized incident to an arrest is . . . simple—get a warrant."[101] Even Justice Alito, who wrote in concurrence and was the sole justice not in the majority, accepted the majority's rule because "we should not mechanically apply the rule used in the predigital era to the search of a cell phone."[102]

Riley was a victory for privacy advocates and an easy case under reasonableness balancing. Upon its release, *Riley* was quickly praised as "a sweeping victory for privacy rights."[103] Some commentators suggested the *Riley* justices would "understand in an immediate sense precisely what it would mean for their privacy if one of their phones was

---

95. *Id.* at 396.
96. *Id.* at 394–96.
97. *Id.* at 393–94. The Court used an instructive analogy in stating:

> [A] cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet.

Id. at 394.
98. *Id.* at 393 (internal citations omitted).
99. *Id.*
100. *Id.* at 386.
101. *Id.* at 403.
102. *Id.* at 406–07 (Alito, J., concurring).
103. Adam Liptak, *Major Ruling Shields Privacy of Cellphones*, N.Y. TIMES, June 25, 2014, http://www.nytimes.com/2014/06/26/us/supreme-court-cellphones-search-privacy.html.

to be taken and searched."[104] Another proclaimed that the Court had "entered the digital age and fundamentally changed how the Constitution protects our privacy."[105] In particular, observers commended the "simple and blunt" rule that "offered such robust Fourth Amendment protection for cell phones."[106]

Riley stands for the proposition this Article argues for in the border context. While an arrestee has diminished privacy interests, that "does not mean that the Fourth Amendment falls out of the picture entirely."[107] This same mantra should hold steady for individuals at ports of entry and exit.[108]

B. *Riley*'s Ripple Effect on the Circuits

Most likely because of the long history of the border search exception and the relative infancy of the digital era, even courts that have extended *Riley* to border searches have not yet been bold enough to even utter the notion that a warrant should be required to perform forensic analysis on electronic devices as part of a border search.[109] Of course, before *Riley*, no courts were bold enough to say warrants should be required incident to a valid arrest. Regardless, *Riley* has led to some decisions that have held that forensic searches fall into the category of "nonroutine," thus, requiring at least some level of suspicion even when conducted as a border search.

1. Properly Applying Riley *to Require At Least Reasonable Suspicion at the Border*

Recently, in *United States v. Kolsuz*, the United States Court of Appeals for the Fourth Circuit held that "in light of the . . . decision in *Riley*, a forensic border search of a phone must be treated as nonroutine,

104. Noah Feldman, *Justices Don't Want Their Smartphones Searched*, BLOOMBERG OPINION, June 25, 2014, 11:24 AM EDT, http://www.bloombergview.com/articles/2014-06-25/justices-don-t-want-their-smartphones-searched.

105. Politico Magazine, *How the Supreme Court Changed America This Year*, POLITICO MAGAZINE, July 1, 2014, http://www.politico.com/magazine/story/2014/07/how-the-supreme-court-changed-america-this-year-108497.html; *see also, e.g.*, Richard Re, *Symposium: Inaugurating the Digital Fourth Amendment*, SCOTUSBLOG (June 26, 2014, 12:37 PM), http://www.scotusblog.com/2014/06/symposium-inaugurating-the-digital-fourth-amendment.

106. Adam Gershowitz, *Symposium: Surprising Unanimity, Even More Surprising Clarity*, SCOTUSBLOG (June 26, 2014, 11:02 AM), http://www.scotusblog.com/2014/06/symposium-surprising-unanimity-even-more-surprising-clarity.

107. *Riley*, 573 U.S. at 392.

108. *See infra* pt. IV.

109. *See* United States v. Molina-Isidoro, 884 F.3d 287, 291 (5th Cir. 2018) (finding nonroutine searches require only reasonable suspicion).

permissible only on a showing of individualized suspicion."[110] The defendant had been detained at Washington Dulles International Airport after federal agents found firearms in his luggage before boarding a flight to Turkey.[111] The agents took possession of the defendant's smartphone and subjected it to an extensive off-site search that produced almost 900 pages of data from the device.[112] The court was explicit in stating that examination of the defendant's phone was a "nonroutine border search, requiring some measure of individualized suspicion."[113] It is important to note that although the court did not agree with the defendant that his particular circumstances were attenuated from the purpose of the border search exception, it specified that there is inherently a point at which the search can be severed from the initial border search.[114]

This holding is at odds with the CBP's Directive that phones can be held indefinitely with supervisory approval.[115] However, there must be some temporal element that severs a search from a border search.[116] The court in *Saboonchi* expressed legitimate concerns over the government's ability to access data indefinitely.[117]

2. The Eleventh Circuit's Failure to Connect Riley to the Border

While some courts have made the connection between *Riley* and border searches, others have refused to move on from predigital doctrines. In *United States v. Touset*, the United States Court of Appeals for the Eleventh Circuit rejected the Fourth and Ninth Circuits' holdings in *Kolsuz* and *Cotterman* and in contrast held that forensic searches of electronic devices at the border are constitutional in the absence of a warrant, probable cause, or individualized suspicion.[118] The court not

110. 890 F.3d 133, 144 (4th Cir. 2018); *see also* United States v. Saboonchi, 48 F. Supp. 3d 815, 819 (D. Md. 2014) (concluding *Riley* confirms that border searches of digital devices are intrinsically nonroutine).

111. *Kolsuz*, 890 F.3d at 136.

112. *Id.*

113. *Id.* at 137.

114. *Id.* at 143.

115. Border Search of Electronic Devices, *supra* note 55, ¶ 5.4.1.1.

116. *See* United States v. Saboonchi, 990 F. Supp. 2d 536, 565–66 (D. Md. 2014) (noting there is a dichotomy between perusing a computer as soon as it crosses the border and using a border crossing as an excuse to obtain a full copy of its contents to scan through in the future).

117. Jared Janes, Comment, *The Border Search Doctrine in the Digital Age: Implications of Riley v. California on Border Law Enforcement's Authority for Warrantless Searches of Electronic Devices*, 35 REV. LITIG. 71, 95 (2016).

118. 890 F.3d 1227, 1229 (11th Cir. 2018); *see also* United States v. Vergara, 884 F.3d 1309, 1312–13 (11th Cir. 2018) (rejecting the warrant requirement, observing that "[b]order searches

only failed to extend *Riley's* warrant requirement, but also held reasonable suspicion is *not* required for forensic searches of electronic devices at the border.[119] It emphasized that a "traveler's 'expectation of privacy is less at the border,'" a constant theme for those who argue the antiquated doctrine should not be reconsidered for electronic devices.[120]

The *Touset* Court argued that it was up to Congress to afford individual privacy more than constitutionally minimal protections.[121] This would seem to suggest that there is no reasonableness test under the Fourth Amendment at the border, and all searches there are automatically constitutional. However, *Flores-Montano* and *Montoya De Hernandez* have already told us that searches that are not routine in nature do require some level of suspicion.[122] Ultimately, the court in *Touset* failed to acknowledge that the Supreme Court had already found a difference between routine and nonroutine searches, and that searches of electronic devices are not routine and do require some level of suspicion to comport with the Fourth Amendment.

There is always the underlying argument that if a person has nothing to hide then they should have no problem letting the government sift through every piece of data on their phone. As one court said: "Laptops and cell phones are indeed becoming quantitatively, and perhaps qualitatively, different from other items, but that simply means there is more room to hide digital contraband, and therefore more storage space that must be searched."[123] Maybe this is so, but the same argument could apply to any illegal search. An innocent person may not be concerned with what might be found in their home by government actors; however, neither the Supreme Court, the legislature, nor the greater American society have ever considered arbitrary searches of homes to be reasonable. Whether a person should have nothing to worry about is irrelevant. What is relevant is the Fourth Amendment to the Constitution that protects from all unreasonable searches.[124]

---

have long been excepted from warrant and probable cause requirements," and concluding that *Riley* "does not change this rule").

119. *Touset*, 890 F.3d at 1232–37.

120. *Id.* at 1235 (quoting United States v. Flores-Montano, 541 U.S. 149, 154 (2004)).

121. *Touset*, 890 F.3d at 1236–37.

122. *Flores-Montano*, 541 U.S. at 155–56; United States v. Montoya De Hernandez, 473 U.S. 531, 541 (1985).

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

124. U.S. CONST. amend. IV.

V. BORDER SEARCHES OF ELECTRONIC DEVICES REQUIRE A WARRANT UNDER THE FOURTH AMENDMENT

The border search exception is a necessary tool to assist government officials in keeping unwanted persons and contraband out of the country; however, it is not an unfettered catch-all that allows officials to disregard Fourth Amendment protections. Reasonableness has always been the touchstone of the Fourth Amendment.[125] In determining reasonableness, it is essential to examine "all of the circumstances surrounding the search or seizure and the nature of the search or seizure itself."[126] At the heart of the Fourth Amendment is a safeguard for the "privacy and security of individuals against *arbitrary* invasions by governmental officials."[127] The Amendment requires a balance that looks to "conserve public interests as well as the interests and rights of individual citizens."[128]

A. Detailed Forensic Analysis of Cell Phones and Other Electronic Devices is Too Far Attenuated from the Border Search Exception's Purpose

It is important to recognize the categories contemplated by Congress when originally granting the authority to conduct border searches without probable cause or a warrant. Goods, wares, or merchandise elicit images of tangible items.[129] Although goods, wares, and merchandise were not defined, this Congress could not have fathomed items like today's electronic devices and the vast amounts of data they can store. Those items originally conceptualized by Congress were physical contraband that could be wholly prevented from entering the border if seized. No such guarantee exists with the ones and zeroes that go into the digital codes that make up the data stored on electronic devices.

Indeed, times change, and doctrines must adjust. The Supreme Court, looking to the considerations for the Fourth Amendment at the time it was enacted, has continually prevented technological advancements from diminishing constitutional protections.[130] The

125. Florida v. Jimeno, 500 U.S. 248, 250 (1991).
126. *Montoya De Hernandez*, 473 U.S. at 537 (citing New Jersey v. T.L.O., 469 U.S. 325, 337 (1985)).
127. Camara v. Mun. Court of S.F., 387 U.S. 523, 528 (1967) (emphasis added).
128. Carroll v. United States, 267 U.S. 132, 149 (1925).
129. *See supra* pt. I.
130. Kyllo v. United States, 533 U.S. 27, 33–34 (2001).

purpose of the border search exception is "grounded in the recognized right of the [United States] to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country."[131] But forensic searches of electronic devices are physically and practically incompatible with this purpose. The data these devices store are not tangible items that can be prevented from entering or exiting the country by a border search. Data can be easily sent to other devices already located in the country without ever being physically transported through a customs checkpoint. There is not a wall that can be built high enough to prevent potential digital contraband from entering or exiting the country.

Remote servers all over the world can store data and transfer it throughout the World Wide Web. The only real reason to search these devices is to extract every piece of information possible about a traveler, not to prevent contraband from crossing border checkpoints. Although this would be a useful tool for law enforcement, so too would allowing police officers to conduct weekly searches of everyone's homes. Indeed, searching electronic devices without a warrant does not comport with the purpose and concept of the Fourth Amendment's border exception.

The Supreme Court has given careful consideration and appropriate weight to the government's use of new and increasingly sophisticated surveillance methods.[132] This consideration reflects the important goal of "assur[ing] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[133] The Court has held that when technology allows law enforcement to access previously unavailable information, due consideration must be given to the corresponding privacy implications.[134] In an era far more advanced than the Founders could

131. United States v. Ramsey, 431 U.S. 606, 620 (1977).

132. Kyllo v. United States, 533 U.S. 27, 36 (2001). *Kyllo*, although not a border case, does support the proposition that the Constitution is not stagnant. *See id.* As new technology is invented, it is imperative that we don't simply fall back on established practices and doctrines that never contemplated such advancements. In *Kyllo*, police used a thermal-imaging device to detect heat emanating outside of the house where petitioner was growing marijuana. *Id.* at 29. The Court ruled the evidence obtained regarding the interior of the home was inadmissible because obtaining that information could not have been gathered without the technology, which was importantly not available to the general public. *Id.* at 40. The Court declined to simply fall back on accepted precedent that there is no expectation of privacy outside of the home, and instead found that reasonable expectation of privacy must adapt with the times. *Id.*

133. *Id.* at 34.

134. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2212–13 (2018) (cell phone records revealing geolocation data); Riley v. California, 573 U.S. 373, 385–86 (2014) (modern cell phone searched incident to arrest); Kyllo, 533 U.S. at 34 (thermal imaging device used to scan a private home); Katz v. United States, 389 U.S. 347, 358 (1967) (listening device on public payphone).

have grasped, electronic devices hold more of the privacies of life than any luggage, package, or even the body can contain. When we marry the original intent of the Fourth Amendment, the purpose of the border search exception, and the capabilities of modern-day technologies, we find that warrants are necessary to perform searches of electronic devices at the border.

The border search exception must stop when searches are no longer serving the purpose of the exception.[135] The Supreme Court has made clear that cell phones are fundamentally different "in both a quantitative and a qualitative sense" from other objects traditionally subject to government searches.[136] It emphasized: "Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[137] The Supreme Court was clear: saying that a search of stored data is "materially indistinguishable" from searches of other physical items, such as a car or suitcase, "is like saying a ride on horseback is materially indistinguishable from a flight to the moon[;] [b]oth are ways of getting from point A to point B, but little else justifies lumping them together."[138]

B. Additional Privacy Infringements That Far Outweigh the Wants of the Government

As the Supreme Court observed, cell phones are "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."[139] Not only are forensic searches of electronic devices outside the bounds of the border search exception, but there are also many deeply concerning privacy issues that are present with electronic devices that are not present with the types of searchable items traditionally encompassed in the border search exception.

---

135. *See* United States v. Kolsuz, 890 F.3d 133, 143 (4th Cir. 2018). The Court remarked:

> Where the government interests underlying a Fourth Amendment exception are not implicated by a certain type of search, and where the individual's privacy interests outweigh any ancillary governmental interests, the government must obtain a warrant based on probable cause. At some point, in other words, even a search initiated at the border could become so attenuated from the rationale for the border search exception that it would no longer fall under that exception.

Id.

136. *Riley*, 573 U.S. at 393.

137. *Id.*

138. *Id.*

139. *Id.* at 385.

Electronic devices truly have become a part of our everyday existences and are relied on for tasks including budgeting, navigating, communicating with foreign language speakers, and countless other needs. Many Americans are not even fully cognizant of what data exists on their phones. Most people understand how to avoid packing unauthorized items in their suitcase before crossing a border, but many do not know how to permanently delete unwanted files from a digital device.[140]

If the Supreme Court or Congress does not act to reestablish reasonableness to the border search exception, the CBP will continue to have unprecedented access into the private lives of every American citizen who leaves the country or returns home—without a scintilla of reason or provocation to do so. Currently, CBP officials can perform an indefinite and practically limitless search of a cell phone with no suspicion at all.[141] Furthermore, this leads to the axiomatic conclusion that the CBP can use "routine searches" to generate reasonable suspicion to conduct a full forensic analysis.

By using sophisticated hacking machines, the government can confiscate electronic devices indefinitely to have access to immense amounts of data that could never be accessed through the searches originally contemplated by Congress.[142] If that were not enough, they can then search out data not even stored on the devices and pillage through a person's privileged information.[143] Although these concerns are covered to some extent by the 2018 CBP Directive, the Directive is a mere agency policy, and CBP made sure to qualify the policy as not constitutionally required.[144] Issuing an agency policy makes it easier for CBP to do as it sees fit. Instead, if the CBP attempted to make it a regulation in the Code of Federal Regulations, the rulemaking process would require a notice and comment period that would likely open the Agency up to much scrutiny. As it stands, the Directive places individual privacies under constant threat.

140. *See generally* Sophia Cope et al., *Digital Privacy at the U.S. Border: Protecting the Data on Your Devices*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/wp/digital-privacy-us-border-2017 (educating travelers on techniques to thoroughly wipe data from their electronic devices) (last visited Aug. 16, 2020).

141. Border Search of Electronic Devices, *supra* note 55, ¶ 5.1.3.

142. Cope, *supra* note 140, at 13, 29.

143. *Id.* at 30.

144. Border Search of Electronic Devices, *supra* note 55, ¶ 4.

1. All Citizens and International Travelers Are Susceptible to Suspicionless Searches

On a typical day in the 2018 fiscal year, CBP officials processed 1,113,914 incoming passengers and pedestrians, including 285,925 private vehicles.[145] For the 2018 fiscal year, there was a record 233.6 million passengers on international flights to and from the United States.[146] This included 93,038,257 American citizens who traveled internationally.[147] Even with the CBP's 2018 Directive requiring reasonable suspicion to conduct a forensic search, those staggering numbers are representative of the amount of travelers susceptible to having their electronic devices searched with no suspicion at all. Of course, CBP believes it can conduct forensic searches of an electronic device at its own discretion at any time.[148]

CBP searched 33,295 devices in the 2018 fiscal year, which was up more than six-fold from 2012.[149] This was a steady increase from previous years. In the 2017 fiscal year, CBP officers conducted 30,200 searches of electronic devices at the border.[150] That represented a sharp increase from the 19,051 searches conducted in fiscal year 2016.[151] These numbers may seem small in comparison to the number of total travelers, but that is 82,546 individuals over the past three years that potentially had the most intimate details of their lives exposed to the government without requiring the government to give a reason. This is akin to the government having drop boxes for cell phones at ports of entry and exit and arbitrarily deciding whose information they will pilfer through and potentially store indefinitely in a government database.

Furthermore, not only are electronic devices often sent to a separate location for forensic analysis, initial searches can be conducted

---

145. *On a Typical Day in Fiscal Year 2018, CBP . . .* , U.S. CUSTOMS & BORDER PROTECTION, https://www.cbp.gov/newsroom/stats/typical-day-fy2018 (last modified Apr. 15, 2020).

146. *2018 Traffic Data for U.S. Airlines and Foreign Airlines U.S. Flights*, U.S. DEP'T OF TRANSP. (Mar. 21, 2019), https://www.bts.gov/newsroom/2018-traffic-data-us-airlines-and-foreign-airlines-us-flights.

147. Nat'l Travel and Tourism Office, *supra* note 3.

148. Border Search of Electronic Devices, *supra* note 55, ¶ 4.

149. Edward C. Baig, *U.S. Customs Can Seize Your Laptop or Phone Without a Warrant. Advocates Cry Foul in Court*, USA TODAY (May 1, 2019, 5:01 AM ET), https://www.usatoday.com/story/tech/2019/05/01/u-s-customs-can-seize-your-phone-when-you-return-home-abroad/3632116002/.

150. *CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics*, U.S. CUSTOMS AND BORDER PROTECTION (Jan. 5, 2018), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and [hereinafter *FY17 Statistics*].

151. *Id.*

well away from a border checkpoint.[152] The search powers of the CBP extend 100 air miles inland from any external boundary of the U.S.[153] This gives border officials the ability to pull over motorists as part of roving border patrol operations.[154] Additionally, CBP may enter onto private land within 25 miles of any external boundary without a warrant.[155]

Even if society were to accept a lower expectation of privacy as they cross the border or get off of an airplane, it is likely that once past that point they would no longer expect to be subject to a search again. The farther an individual is from the border, the more likely it is his or her expectation of privacy would increase. Conducting these searches tens of miles away from the border may be an important tool for the CBP to conduct their mission, but it further illustrates that the expectation of privacy in one's electronic device well away from a port of entry or exit is even greater and should require a warrant.

Nearly two out of three American citizens live within the 100-mile border zone.[156] New Jersey, Delaware, Vermont, Hawaii, Rhode Island, Massachusetts, New Hampshire, Connecticut, New York, Maine and Florida lie entirely or almost entirely within the 100-mile border zone.[157] Moreover, "[n]ine of the ten largest U.S. metropolitan areas, as determined by the 2010 Census, also fall within this zone: New York City, Los Angeles, Chicago, Houston, Philadelphia, Phoenix, San Antonio, San Diego and San Jose."[158]

It is easy to be indifferent and pass off this constitutional infringement by focusing on the small overall percentage of citizens who had their rights violated—unless of course you are one of the tens of thousands of people annually whose most intimate conversations, pictures, and life details were arbitrarily exposed to a government agent for no reason at all. For those individuals, the dignity and privacy infringements are as real as any search of the home.[159] This "police

152. Border Search of Electronic Devices, *supra* note 55, ¶ 5.4.1; Patrick G. Lee, *Can Customs and Border Officials Search Your Phone? These Are Your Rights*, PROPUBLICA (Mar. 13, 2017, 12:55 PM EDT), https://www.propublica.org/article/can-customs-border-protection-search-phone-legal-rights.

153. Lee, *supra* note 152.

154. *Id.*

155. *Id.*

156. *The Constitution in the 100-Mile Border Zone*, ACLU, https://www.aclu.org/other/constitution-100-mile-border-zone (last visited Aug. 17, 2020).

157. *Id.*

158. *Id.*

159. *See* Seth Harp, *I'm a Journalist but I Didn't Fully Realize the Terrible Power of U.S. Border Officials Until They Violated My Rights and Privacy*, THE INTERCEPT (June 22, 2019, 8:00 AM), https://theintercept.com/2019/06/22/cbp-border-searches-journalists/. Consider the three-

state"[160] type practice cannot meet the reasonableness test of the Fourth Amendment or the original intent of the Founders.

2. Cloud-Based Access

The Supreme Court has never considered the category of electronic devices under the border search exception; however, the CBP currently believes it has the implicit authority to access passwords and remote storage platforms when it conducts forensic searches.[161] If the device is connected to the cloud, then the investigator has virtually unlimited access to a person's digital existence.[162] This means that now the search would extend well past the physical property carried across the border and into files located at remote servers which could be located anywhere in the world. "While [electronic devices] are compact at a physical level, every computer is akin to a vast warehouse of information."[163]

3. Privileged Information

The border search exception puts unsuspecting travelers at risk—including "lawyers who need to protect attorney-client privilege,

---

hour encounter Mr. Harp, a United States citizen, encountered when CBP officials confiscated his phone:

> After I gave him the password to my iPhone, Moncivias spent three hours reviewing hundreds of photos and videos and emails and calls and texts, including encrypted messages on WhatsApp, Signal, and Telegram. It was the digital equivalent of tossing someone's house: opening cabinets, pulling out drawers, and overturning furniture in hopes of finding something — anything — illegal. He read my communications with friends, family, and loved ones. He went through my correspondence with colleagues, editors, and sources. He asked about the identities of people who have worked with me in war zones. He also went through my personal photos, which I resented. Consider everything on your phone right now. Nothing on mine was spared.

Id.

160. A "police state" is defined as: "[A] political unit characterized by repressive governmental control of political, economic, and social life usually by an arbitrary exercise of power by police and especially secret police in place of regular operation of administrative and judicial organs of the government according to publicly known legal procedures." *Police State*, MERRIAM-WEBSTER DICTIONARY, https://www.merriam-webster.com/dictionary/police%20state (last visited Aug. 17, 2020) (emphasis added).

161. *See* Border Search of Electronic Devices, *supra* note 55, ¶ 5.3.1.

162. This is a concern the CBP has acknowledged: "[One] privacy risk concerns CBP's potential over-collection of information from individuals due to the volume of information that is either stored on, or accessible by, today's electronic devices." *Privacy Impact Assessment Update for CBP Border Searches of Electronic Devices DHS/CBP/PIA-008(a)*, U.S. DEP'T OF HOMELAND SEC. (Jan. 4, 2018), https://www.dhs.gov/sites/default/files/publications/PIA-CBP%20-%20Border-Searches-of-Electronic-Devices%20-January-2018%20-%20Compliant.pdf.

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

business people with proprietary information, researchers who promise their subjects anonymity, and photojournalists who may pledge to blur a face to conceal an identity."[164] The government's practices open up the very real possibility that individuals with sensitive data on their phone will have to inappropriately expose the data to border officials.[165] These privacy infringements cannot be undone. It is noble to think that law enforcement officials will forget what they see and stay within the confines of their jurisdiction; however, this puts too much temptation in the hands of individuals motivated to pursue crimes. It seems likely that searches occur without the traveler knowing what the appropriate procedures are. Many travelers would feel compelled to hand over their devices to officers if asked.[166] Indeed, law enforcement officials have

164. Sean O'Grady, *All Watched Over by Machines of Loving Grace: Border Searches of Electronic Devices in the Digital Age*, 87 FORDHAM L. REV. 2255, 2257 (2019).

165. The CBP does have a somewhat convoluted policy in place to try and attempt to mitigate these risks. For example, for attorney-client privileged data, the Directive states:

> 5.2.1.1 The Officer shall seek clarification, if practicable in writing, from the individual asserting this privilege as to specific files, file types, folders, categories of files, attorney or client names, email addresses, phone numbers, or other particulars that may assist CBP in identifying privileged information.
>
> 5 .2.1.2 Prior to any border search of files or other materials over which a privilege has been asserted, the Officer will contact the CBP Associate/ Assistant Chief Counsel office. In coordination with the CBP Associate/ Assistant Chief Counsel office, which will coordinate with the U.S. Attorney's Office as needed, Officers will ensure the segregation of any privileged material from other information examined during a border search to ensure that any privileged material is handled appropriately while also ensuring that CBP accomplishes its critical border security mission. This segregation process will occur through the establishment and employment of a Filter Team composed of legal and operational representatives, or through another appropriate measure with written concurrence of the CBP Associate/ Assistant Chief Counsel office.

Border Search of Electronic Devices, *supra* note 55, ¶¶ 5.2.1.1–5.2.1.2. The Directive also states procedures for dealing with other possibly sensitive material. *Id.* ¶ 5.2.2.

166. *See* Kaveh Waddell, *A NASA Engineer Was Required to Unlock His Phone at the Border*, THE ATLANTIC (Feb. 13, 2017), https://www.theatlantic.com/technology/archive/2017/02/a-nasa-engineer-is-required-to-unlock-his-phone-at-the-border/516489/. The author tells the story of Sidd Bikkannavar, a U.S.-born citizen, returning from two-week trip to Chile:

> But the agent never touched Bikkannavar's bag—instead, he asked for his smartphone. Bikkannavar handed it over, assuming the agent might just want to inspect it to make sure it wasn't something more dangerous in disguise. The agent turned it over in his hand and asked for the passcode.
>
> Bikkannavar was taken aback. The phone was Jet Propulsion Lab property, he explained, pointing out the barcode stuck to the back. It was his duty to protect its sensitive contents, and he couldn't give out the passcode.
>
> . . .

ordered border searches of travelers' devices to gather evidence of crimes unrelated to the import or export of contraband.[167] It does not take a large leap to conclude that suspicion of law enforcement is why the Fourth Amendment exists.

4. Indefinite Confiscation and Detention of Data

As discussed earlier in this Article,[168] there is no restriction on the amount of time the CBP may confiscate or perform forensic analysis on an electronic device. Even if the border search exception were to permit the initial seizure of an electronic device without any suspicion present, the "[g]overnment cannot simply seize property under its border search power and hold it for weeks, months, or years on a whim."[169]

Under CBP policy, confiscation ordinarily should not exceed five days but can be prolonged indefinitely with a supervisor's approval.[170]

> Bikkannavar didn't feel like he had a choice. "I'd read the headlines of people being stranded in airports and having problems entering the country, so I was still in the mode of being as cooperative and polite and courteous as possible," he said to me.

Id.

167. *See, e.g.*, United States v. Kim, 103 F. Supp. 3d 32, 46 (D.D.C. 2015) (describing a border search of a laptop as "nothing more than a fishing expedition to discover what [the traveler] might have been up to"). *See also*, Matthew S. Schwartz, *ACLU: Border Agents Violate Constitution When They Search Electronic Devices*, NPR (May 2, 2019, 5:10 AM ET), https://www.npr.org/2019/05/02/719337356/aclu-border-agents-violate-constitution-when-they-search-electronic-devices (discussing the border search exception and the American Civil Liberty Union's (ACLU) findings through depositions of CBP agents that "warrantless searches has expanded far beyond the mere enforcement of immigration and customs laws").

168. *See supra* pt. II.

169. House v. Napolitano, No. 11-10852-DJC, 2012 U.S. Dist. LEXIS 42297, at *28 (D. Mass. Mar. 28, 2012) (quoting United States v. Cotterman, 637 F.3d 1068, 1070 (9th Cir. 2011)). In *House*, the Defendant's laptop was seized for 49 days by border officials. *Id.* at *2. The court held that the seizure had to be reasonably related in scope to why it was originally seized. *Id.* at *29. *See also Cotterman*, 637 F.3d at 1082–83 (finding a two-day seizure of an electronic device as a part of a border search was reasonable, but only after a full account of what the government was doing with the laptop to ensure that it was performing its duties responsibly).

170. Border Search of Electronic Devices, *supra* note 55, ¶ 5.4.1. The Directive states:

> Approval of and Time Frames for Detention. Supervisory approval is required for detaining electronic devices, or copies of information contained therein, for continuation of a border search after an individual's departure from the port or other location of detention. Port Director; Patrol Agent in Charge; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or other equivalent level manager approval is required to extend any such detention beyond five (5) days. Extensions of detentions exceeding fifteen (15) days must be approved by the Director, Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or other equivalent manager, and may be approved and re-approved in increments of no more than seven (7) days. Approvals for detention and any extension thereof shall be noted in appropriate CBP systems.

This means that a government official may confiscate any American citizen's phone, possibly for the entirety of their trip, for forensic analysis while they go on a family vacation overseas. Furthermore, this confiscation is subject only to the requirement of reasonable suspicion under the current CBP policy—or no suspicion at all under the Agency's general interpretation of caselaw.[171] These standards do not pass the reasonableness test of the Fourth Amendment nor the balancing of the rights of citizens and government interests. Such a practice could not have been the intention of the Congress who authorized the searches of cargo entering on ships back in the 1700s.

C. Legislative Recognition of the Abuse of Power

Recent court cases and outside influences have brought the issue to the attention of Congress—and members are taking action to correct this constitutional infringement. Versions of the "Protecting Data at the Border Act" have been introduced in both the House of Representatives and the Senate.[172] In an age with incredibly divisive political discourse and partisanship, it is noteworthy that these were bicameral, bipartisan bills. The bills were introduced by Congressman Ted W. Lieu (D-Los Angeles County), Sen. Ron Wyden (D-Oregon), Sen. Rand Paul (R-Kentucky), Sen. Edward Markey (D-Massachusetts), and Sen. Jeff Merkley (D-Oregon).[173]

The bills have provisions that are congruent with the arguments made in this Article. First, the bill

> prohibits a governmental entity from: (1) accessing the digital contents of electronic equipment belonging to, or in the possession of a U.S. person (person) at the border without a valid warrant; or (2) denying a person's U.S. entry or exit based on the person's refusal to disclose an access credential or in order to determine whether such person will consensually provide an access credential, access, or online account information.[174]

Id. ¶ 5.4.1.1.

171. *Id.* ¶ 4.

172. *Rep. Lieu and Senators Introduce Bicameral Bill to Protect the Privacy of Americans at the U.S. Border*, TED LIEU (May 22, 2019), https://lieu.house.gov/media-center/press-releases/rep-lieu-and-senators-introduce-bicameral-bill-protect-privacy-americans [hereinafter *Rep. Lieu Press Release*].

173. *Id.*

174. Congressional Research Service, *S.823 - Protecting Data at the Border Act*, CONGRESS.GOV, https://www.congress.gov/bill/115th-congress/senate-bill/823 (last visited Aug. 8, 2020).

Second, the bill still allows border officials to "access the digital contents of electronic equipment without a warrant if the officer determines that an emergency situation exists."[175]

The "officer must subsequently apply for a warrant within seven days, and if such warrant is not granted: (1) digital content copies must be destroyed, (2) digital contents or information may not be disclosed, and (3) the person shall be notified of such destruction."[176] In addition, the bill establishes that a "governmental entity may not make or retain a copy of the digital contents of electronic equipment, an online account, or online account information without probable cause to believe that such information contains evidence of, or constitutes the fruits of, a crime."[177]

These are constitutionally appropriate guidelines that would ensure that the CBP is truly conducting searches judiciously, responsibly, and consistent with public trust. Moreover, requiring a warrant for searches of data on electronic devices is the standard the Fourth Amendment requires—as is explicitly acknowledged in the bills and by their authors.[178]

Currently these bills are still sitting in subcommittee and hearings have been held.[179] These bills are a great step in the right direction;

---

175. *Id.*
176. *Id.*
177. *Id.* Furthermore, the bills would make the following law:

> Unlawfully accessed information: (1) must be destroyed and the person notified of its destruction; (2) may not be disclosed; and (3) may not be received in evidence in any trial, hearing, or other proceeding.
>
> A governmental entity shall keep a record of each instance in which it obtains access to an individual's digital information.
>
> A governmental entity may not seize electronic equipment belonging to, or in the possession of, a person at the border without probable cause to believe that such equipment contains information relevant to a felony.

Id.

178. Upon introduction for the House bill, Rep. Lieu said:

> We must protect Americans' privacy—whether it's on a city sidewalk, at a border checkpoint or anywhere else in the U.S. At the border, American travelers should not be subjected to invasive searches of their electronic devices without a warrant. The Fourth Amendment guarantees this right. I'm proud to introduce the House version of Senators Wyden and Paul's bipartisan bill to ensure that the rights of Americans are protected and that the government does not indiscriminately search the phones and laptops of Americans without cause.

Rep. Lieu Press Release, *supra* note 172.

179. Congressional Research Service, *supra* note 174.

however, they are just bandaging a constitutional infringement. Regardless of whether these bills are passed, the Supreme Court must bring finality to the issue by deeming warrantless searches of electronic devices unconstitutional. The whims of Congress are too tenuous to trust that the same policies that have been allowed to fester for too long will not be reimplemented when it is politically convenient. Indeed, even if Congress passes the aforementioned bills, the Supreme Court should drive the proverbial nail in the coffin of improper government intrusion into Americans' electronic devices without a warrant.

D. Protecting Constitutional Rights Does Not Prevent CBP from Meeting Its Mission

Requiring the government to abide by the Constitution and protect the privacy interests of unsuspecting citizens does not diminish the ability of the CBP to do its job any more than preventing law enforcement from taking daily tours of a known criminal's house without probable cause affects its mission. Indeed, if we all decided to let law enforcement have unlimited access to everyone's personal information at law enforcement's whim, inevitably more crimes would be discovered, but at an intolerable price.

The Fourth Amendment provides "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no [w]arrants shall issue, but upon probable cause."[180] The privacy rights of citizens overpower the convenience of the government.

Nothing about a warrant requirement for searches of electronic devices would prevent border agents from stopping every traveler they so desired and conducting searches traditionally covered under the border search exception. CBP emphasizes that only 0.007 percent of incoming passengers have their devices searched to demonstrate that a low number of individuals undergo these searches when compared to the number of people crossing the border.[181] That means 99.993 percent of the time, requiring a warrant of CBP would have zero effect on the Agency—and the remaining percentage of time it can get a warrant. Indeed, if during a stop, probable cause develops to suspect an individual of a crime, the device may be seized at the border and detained pending

180. U.S. CONST. amend. IV.
181. *FY17 Statistics*, *supra* note 150.

an officer's "reasonable steps to secure" and "preserve evidence while they awaited a warrant."[182]

Furthermore, the government inherently has the right to protect citizens against imminent danger without having to first get a warrant when ordinarily required. "Such exigencies include the need to pursue a fleeing suspect, protect individuals who are threatened with imminent harm, or prevent the imminent destruction of evidence."[183]

VI. CONCLUSION

The Supreme Court acknowledged in *Riley* that cell phones have a vastly greater capacity to store information and would expose more of an individual's private information than a home ever could.[184] The Court correctly stated:

> [A] cell phone search would typically expose to the government *far more than the most exhaustive search of a house*: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form-unless the phone is.[185]

In *United States v. Kirschenblatt*, Learned Hand noted that it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him."[186] In today's context, electronic devices often carry far more personal data than can be obtained by ransacking a person's home. The Supreme Court has held that reasoning applying the Fourth Amendment to digital property must "rest on its own bottom."[187] Because electronic devices, like cell phones, can handle such immense amounts of private data that falls outside the purpose of the border search exception, these devices require due protection.

In order for constitutional protections to apply, an individual's expectation of privacy in the object of the search must be one that

182. Helen Hong, *Border Searches of Digital Devices*, 67 DOJ J. FED. L. & PRAC. 199, 212 (2019).

183. Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018). The *Carpenter* Court held that the government does not have "unrestricted access to a wireless carrier's database of physical location information." *Id.* The reasoning was because of the "[d]eeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection." *Id.* However, the Court recognized that there still remained exigent circumstances when the government may discard the requirement to secure a warrant. *Id.*

184. Riley v. California, 573 U.S. 373, 396 (2014).

185. *Id.* at 396–97 (emphasis added).

186. 16 F.2d 202, 203 (2d Cir. 1926).

187. *Riley*, 573 U.S. at 393.

"society is prepared to recognize as reasonable."[188] The highly intrusive nature of confiscating a device, for possibly weeks at a time, and subsequent use of a hacking machine to uncover every piece of data off of it is hardly one most Americans would find reasonable. Electronic devices should garner the same protections as they do with other exceptions to the Fourth Amendment—specifically, a warrant. The warrant requirement is "an important working part of our machinery of government," not merely "an inconvenience to be somehow 'weighed' against the claims of police efficiency."[189]

The long-held tradition of allowing warrantless searches of other types of property is unquestionably an important part of keeping contraband out of the interior. Furthermore, this Article does not mean to completely disregard the argument that procuring warrants for searches of cell phones and other electronic devices will take time and resources away from the CBP. However, there is a point where any search can go too far. Requiring a warrant to obtain the highly sensitive and exorbitant amounts of data that can be stored on electronic devices would produce the proper balance that the Fourth Amendment mandates between the rights of the people and the interests of the government. The alternative would condone a reality where anyone entering or exiting the United States must accept the possibility that their entire digital existence could be scrutinized by the government with no justification necessary for the government's actions. This does invoke the dignity and privacy concerns that make the warrant requirement appropriate regarding border searches—as these dignity and privacy concerns with searches of electronic devices have been found in every other context.

The Supreme Court and Congress must act immediately to stop the unconstitutional practice of searching electronics at the border without a warrant. Until this happens, every traveler entering or exiting the country should take extreme precaution on what information is stored on their devices. Unfortunately, until the Supreme Court or Congress definitively acts, all travelers remain susceptible to their sensitive data being exposed without the government having any reasonable suspicion to do so.[190]

188. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
189. Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971).
190. *See* Matt Novak, *9 Horror Stories from People Who Had Their Electronic Devices Searched at the Border*, GIZMODO (Oct. 9, 2017, 7:45 AM), https://gizmodo.com/9-horror-stories-of-people-who-had-their-electronic-dev-1818730022.