NOTE

DO SOMETHING ALREADY: WHY CONGRESS SHOULD RESOLVE HOW THE BORDER SEARCH DOCTRINE APPLIES TO DIGITAL DEVICES

*Zev T. Chabus**

The proliferation of digital devices, such as smartphones and laptops, in recent years has led to unresolved legal issues involving searches of such devices at United States border crossings. Currently, four federal Circuit Courts of Appeals are split as to when the border search doctrine, which obviates the need for a search warrant at border crossings, allows border agents to search digital devices and when such a search is considered "unreasonable" under the Fourth Amendment. This Note argues that Congress should resolve this issue by enacting a statute with a reasonable suspicion standard or delineating clear circumstances under which it is permissible for border agents to search digital devices. Furthermore, given the sensitivity of information that many people store on digital devices, any such statute should also include strong privacy protections. This Note explores the approaches of the four circuit courts that have ruled on this issue and examines solutions proposed by legal scholars and politicians. In light of the Supreme Court's denial of certiorari on October 5, 2020, to a case that could have resolved this issue, this Note explains why Congress, not the Supreme Court, is best suited to solving this problem.

* B.A., Queens College, City University of New York, 2017; J.D., Cornell Law School, 2022. Thank you to the staff of the *Cornell Journal of Law and Public Policy* for their work on this Note, as well as Sarah St.Vincent for providing insight into unresolved legal issues involving privacy and technology.

INTRODUCTION

The Fourth Amendment is one of the hallmarks of the Constitution. It prohibits any "unreasonable" searches by the government.[1] Before searching someone's property or possessions, the government must obtain a search warrant.[2] However, this requirement is subject to certain exceptions.[3]

On July 31, 1789, Congress decided that searches performed at the border are inherently reasonable.[4] Since the Fourth Amendment requires a warrant only for unreasonable searches, the government does not need a warrant to search someone's property at a border crossing.[5] This became the border search exception, or border search doctrine.[6] The circuit courts are divided over how this exception applies to digital devices.[7] On October 5, 2020, the Supreme Court denied certiorari to a case that could have resolved a four-way circuit split about whether—and, if so, how—the border search exception applies to digital devices.[8]

Part I of this Note will explore the application of the border search exception in each of the relevant four circuits. Part II will examine the scholarly literature about how courts should resolve this issue, including suggestions for a balancing test, warrant requirement, or court-mandated

---

1 U.S. CONST. amend. IV.

2 Katz v. United States, 389 U.S. 347, 357 (1967).

3 *See, e.g.*, Brigham City v. Stuart, 547 U.S. 398, 403 (2006) (searches made in rendering emergency aid); Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973) (consent searches); United States v. Robinson, 414 U.S. 218, 224 (1973) (searches incident to lawful arrests).

4 Act of July 31, 1789, ch. 5, §§ 23–24, 1 Stat. 29, 43.

5 *See Border Searches*, LEGAL INFO. INST., https://www.law.cornell.edu/constitution-conan/amendment-4/border-searches (last visited July 20, 2021).

6 *See, e.g.,* United States v. Cano, 934 F.3d 1002, 1010–11 (9th. Cir. 2019).

7 *See* United States v. Kolsuz, 890 F.3d 133, 144 (4th Cir. 2018); *Cano*, 934 F.3d at 1020; United States v. Rascon-Ortiz, 994 F.2d 749, 752 n.3 (10th Cir. 1993); United States v. Touset, 890 F.3d 1227, 1233 (11th Cir. 2018).

8 *See generally* United States v. Williams, 942 F.3d 1187 (10th Cir. 2019), *cert. denied,* 141 S. Ct. 235 (2020).

reasonable suspicion standard or lack thereof. Part III will argue that Congress, not the courts, should resolve this issue by passing a statute imposing some sort of reasonable suspicion requirement or clear list of appropriate circumstances in which to conduct a search, along with strong protections over how that data should be stored. Finally, Part IV will explore the relevant issues for digital devices and privacy today, like the growing use of digital devices to store sensitive data, and explain why privacy protections are important for any statute that Congress would pass to address this issue.

I

Under the Fourth Amendment, the government must obtain a search warrant before conducting certain "searches and seizures."[9] However, Congress passed a law that declares that searches performed at the border are inherently reasonable and do not require a search warrant.[10]

That exception has been used to search people's possessions at airports in modern times.[11] However, various circuit courts apply the exception in different ways when it comes to forensically searching people's phones.[12]

The Fourth Circuit holds that a forensic search of someone's phone at the border requires an individualized suspicion that that person committed a crime.[13] In *United States v. Kolsuz*, Customs and Border Protection (CBP) agents searched defendant Kolsuz's checked bags when Kolsuz arrived at Dulles Airport en route to Turkey on February 2, 2016.[14] When the CBP agents found firearm parts in Kolsuz's bags, they took Kolsuz to a separate area and searched his phone.[15] The agents looked through Kolsuz's calls and texts.[16] One of the agents then decided to conduct a more detailed, forensic search and sent Kolsuz's phone to a Homeland Security Investigations (HSI) office in Virginia, where they extracted detailed information from the phone.[17] The court found that since the HSI analysts searched Kolsuz's phone at least partly to find

---

9 U.S. CONST. amend. IV; Katz v. United States, 389 U.S. 347, 357 (1967).

10 Act of July 31, 1789, ch.5, §§ 23-24, 1 Stat. 29, 43.

11 *See Border Searches*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/issues/border-searches (last visited Apr. 19, 2021).

12 *See Kolsuz*, 890 F.3d at 144; *Cano*, 934 F.3d at 1020; *Rascon-Ortiz*, 994 F.2d at 752 n.3; *Touset*, 890 F.3d at 1233.

13 *See Kolsuz*, 890 F.3d at 144, 138 ("Thus, with respect to [ ] searches, the border search exception is justified by the government's power to regulate the export of currency and other goods" and that power "surely extends to controls on the exports of dangerous weapons . . . .") (citing United States v. Oriakhi, 57 F.3d 1290, 1296–97 (4th Cir. 1995).

14 *Id.* at 139.

15 *Id.*

16 *Id.*

17 *Id.*

information about an ongoing crime of which Kolsuz was suspected, it was allowed because it "fit[ ] within the core . . . rationale" of the border search exception.[18] The court also found that under *Riley v. California*,[19] a forensic search of a phone, such as the one belonging to Kolsuz, requires a showing that the individual involved is suspected of committing a crime.[20] The court found that there was an adequate showing here.[21]

The Ninth Circuit holds that a forensic border search of someone's phone requires reasonable suspicion that the device contains contraband.[22] On July 25, 2016, when defendant Cano tried to enter the United States from Mexico, CBP agents found cocaine underneath his truck.[23] HSI agents then searched Cano's phone to try to find other evidence of contraband crossing the border.[24] The court found that although the border search exception only applies to searches for contraband, the exception also encompasses digital contraband, not just physical items like drugs.[25] The court reasoned that since the phone itself is physical and there is "the possibility that the phone's contents can be printed or shared electronically," phones are subject to the border search doctrine.[26]

The Tenth Circuit holds that detention at the border requires reasonable suspicion that "an individual is involved in some criminal activity."[27] On October 13, 1991, border patrol agents detained appellee Rascon-Ortiz when he crossed from Mexico to the United States.[28] The agent thought that Rascon-Ortiz was involved in criminal activity because Rascon-Ortiz appeared visibly nervous and was driving a car that was similar to ones previously found to have held contraband.[29] The agent looked under the car at the gas tank and, upon discovering evidence of a false compartment, "brought out a trained dog which alerted on the gas tank."[30] According to the court, "[this] brief visual examination of the vehicle's undercarriage was not a search," given that "[the] undercarriage is part of the car's exterior, and as such, is not afforded a reasonable expectation of privacy."[31] Regardless, the court said that border patrol agents can subject people to nonroutine questioning as long as

---

18 *Id.* at 144.
19 573 U.S. 373 (2014).
20 *See* Kolsuz, 890 F.3d at 144.
21 *Id.*
22 *See* United States v. Cano, 934 F.3d 1002, 1020 (9th Cir. 2019); United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013).
23 *See* Cano, 934 F.3d at 1007.
24 *See id.*
25 *See id.* at 1014.
26 *See id.*
27 United States v. Rascon-Ortiz, 994 F.2d 749, 752 n.3 (10th Cir. 1993).
28 *See id.* at 750.
29 *Id.*
30 *Id.* at 751.
31 *Id.* at 754.

there is a "basis of reasonable suspicion that a crime has been committed."[32] The court said that this reasonable suspicion standard is objective, "[requiring] police to have an articulable, individualized, [and] reasonable suspicion that an individual is involved in some criminal activity."[33]

The Eleventh Circuit, on the other hand, holds that there is no reasonable suspicion requirement at all for searches performed on digital devices at the border.[34] On December 21, 2014, CBP agents inspected defendant Karl Touset's phones and other electronic devices at an Atlanta airport where Touset had arrived on an international flight.[35] The CBP returned the iPhones but kept laptops, hard drives, and tablets for forensic searches.[36] The Department of Homeland Security (DHS) found child pornography on the detained devices and obtained a warrant to search Touset's home.[37] In upholding the validity of the warrant, the court distinguished between searching a person and searching property, in part on the basis of applicable Supreme Court precedent.[38] While the Supreme Court has articulated the need for reasonable suspicion before detaining a person at the border,[39] it has never expressed such a requirement for searches of property at the border.[40] Therefore, the court here decided that since there is no reasonable suspicion requirement for property, and since digital devices constitute property, there is no need to require reasonable suspicion before border agents can search digital devices at the border.[41]

II

Various scholars have proposed solutions to the gap in jurisprudence over border searches of electronic devices. While some scholars support specific measures to protect against such searches, at least one author favors the Eleventh Circuit's approach requiring no reasonable suspicion.[42]

---

32 *Id.* at 752.

33 *Id.* at 752 n.3.

34 United States v. Touset, 890 F.3d 1227, 1233 (11th Cir. 2018).

35 *Id.* at 1230.

36 *Id.*

37 *Id.*

38 *See id.* at 1233–34.

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

40 Touset, 890 F.3d at 1233–34.

41 *Id.*

42 *See, e.g.,* Caroline V. McCaffrey, *Fairly Exposed: A Proposal to Improve the Reasonableness Standard for Digital Forensic Searches at the Border*, 80 LA. L. REV. 202 (2019); Gina R. Bohannon, *Cell Phones and the Border Search Exception: Circuits Split Over the Line Between Sovereignty and Privacy*, 78 MD. L. REV. 563, 603 (2019); Tom Rechtin, *Back to the Future of Your Laptop: How Backlash Over Prolonged Detention of Digital Devices in Border Searches is Symptomatic of a Need for "Reasonable Suspicion" in All Border Searches of Digital Devices*, 7 IDAHO CRITICAL LEGAL STUD. J. 66 (2014); Michael Creta, *A Step in the*

A. The Multi-Factor Balancing Test

Caroline V. McCaffrey has proposed that the courts adopt a multi-factor balancing test.[43] McCaffrey says that a reasonableness standard applies regardless of whether border patrol agents conduct digital forensic searches based on "reasonable suspicion of criminal activity or no suspicion at all."[44] She asserts that this reasonableness standard "involves balancing the need for a search against an individual's reasonable privacy interests," but that is not practical and has led to inconsistent law in this area.[45] She argues that the solution is a multi-factor balancing test that courts can apply on a case-by-case basis instead of deciding cases based on what she terms "courts' personal opinions."[46]

This test has three factors to balance, each of which contains sub-factors. The factors include the (1) duration and (2) procedure of the search, balanced against (3) the harms that would be prevented by conducting the search.[47]

The duration factor includes as sub-factors: the behavior of the CBP agent during the search, especially the diligence of the agent in conducting the search, such as taking reasonable care to avoiding harming the person or device; whether CBP agents gave enough information to the suspect about the amount of time and why their devices were being searched; and the number of CBP agents who would conduct the search, with an eye toward shortening the required time frame for the search.[48]

The procedure factor includes the following sub-factors: the vigilance as to the discretion over what to search, with an eye toward preventing abuse; and methods to limit the amount of discretion that agents have, with an emphasis on notice to travelers.[49] The harms factor contains a two-part analysis: (1) whether agents have facts to believe that a specific individual poses a threat; and (2) whether a forensic search was necessary in order to stop that harm from occurring.[50]

Wrong Direction: The Ninth Circuit Requires Reasonable Suspicion for Forensic Examinations of Electronic Storage Devices During Border Searches in United States v. Cotterman, 55 B.C. L. REV. 31 (2014), https://lawdigitalcommons.bc.edu/bclr/vol55/iss6/4/.

43 McCaffrey, *supra* note 42, at 240.

44 *Id.* at 239.

45 *Id.* at 240.

46 *Id.*

47 *Id.*

48 *Id.* at 241–42.

49 *Id.* at 242–44.

50 *Id.* at 244.

B. The Warrant Requirement

Gina R. Bohannon has proposed that there should be a warrant requirement for these searches.[51] She takes issue with the Eleventh Circuit's distinction between searching a person and searching property and argues that searching someone's phone can result in the same kind of indignity as searching the person directly.[52] She says that the Supreme Court, in *Riley* and *Carpenter v. United States*,[53] recognized that cell phones are worthy of different considerations than would normally apply to other forms of property.[54] She further contends that the purpose of the border search exception is limited in scope, and brings support from cases where the Supreme Court upheld searches for physical contraband.[55] Based on this, Bohannon argues that searching a phone might result in finding digital contraband, such as child pornography, but that is not the same as physical contraband, which she contends is the true focus of the purpose behind the border search doctrine.[56] She argues that in light of these factors, a warrant would best protect people's privacy interests.[57]

There has been a push in Congress for a bill that would require a warrant for these kinds of searches.[58] In 2019, Senators Ron Wyden and Rand Paul introduced the Protecting Data at the Border Act.[59] The bill was designed to prevent law enforcement agencies from searching Americans' cell phones and laptops at the border under the border search exception.[60] Wyden and Paul claimed that the push for the bill was based on the increase of such searches, and that such searches targeted those who were not suspected of crimes, including journalists and activists.[61]

---

51 Bohannon, *supra* note 42, at 603.

52 *Id.* at 592–93.

53 138 S. Ct. 2206 (2018).

54 Bohannon, *supra* note 42, at 593.

55 *Id.* at 594–96 (citing, e.g., United States v. 12 200-Ft. Reels of Super 8mm. Film, 413 U.S. 123, 124–25) (discussing the power of the Secretary of the Treasury to ban the importation of certain books and other physical materials); United States v. Thirty-Seven (37) Photographs, 402 U.S. 363, 376 (1971) (discussing the search of travelers' luggage for contraband); United States v. Ramsey, 431 U.S. 606, 619–20 (upholding the search of physical mail under the border search exception).

56 *Id.* at 596–97.

57 *Id.* at 602.

58 *See* Press Release, Ron Wyden & Rand Paul, Wyden, Paul Bill Requires Warrants to Search Americans' Digital Devices at the Border (May 22, 2019), https://www.wyden.senate.gov/news/press-releases/wyden-paul-bill-requires-warrants-to-search-americans-digital-devices-at-the-border.

59 *Id.*

60 *Id.*

61 *Id.*

Wyden and Paul also cited *Riley*'s support for special consideration of digital data.[62]

C. This Lack of Uniform Jurisprudence has Practical Implications

While other scholars focus on the general implications of the border search exception, Tom Rechtin discusses how a reasonable suspicion standard for border searches of electronic devices is particularly important in the case of international emails.[63] Rechtin first argues that emails should not be subject to the border search doctrine simply because the border search doctrine was not intended to apply to words, which would be the primary contents of an email.[64] Rechtin supports this by saying that the ability to conduct warrantless searches is primarily used by border agents for physical items posing "physical threats."[65] He connects all of this to the requirement of "reasonable suspicion" before searching physical mail, as a lesser standard would interfere with people's privacy rights.[66] Rechtin asserts that the border search doctrine does not apply to emails in particular because they are not physical objects that cross a physical border.[67] Rechtin then says that in light of the issues inherent in email and digital communication, all searches of digital devices at the border should be subject to a reasonable suspicion standard.[68]

D. Do We Really Need a Standard Here?

While much of the literature is in favor of a warrant requirement or at the very least some sort of reasonable suspicion standard articulated by the courts, there are those who would prefer the approach of the Eleventh Circuit and have no reasonable suspicion standard at all.[69] Michael Creta argues that a reasonable suspicion standard would do more harm than good.[70] Creta says that without some sort of suspicion-based standard, there is no need to "creat[e] . . . arbitrary distinctions between different types of property,"[71] as the Ninth Circuit arguably did in *United States v. Cotterman*.[72] Creta maintains that courts should instead look at how searches are conducted, rather than whether the object is physical or digital.[73] Creta argues that a lack of a reasonable suspicion standard is a

---

62 *Id.*
63 Rechtin, *supra* note 42, at 71–72.
64 *See id.* at 84.
65 *See id.*
66 *Id.* at 83–84.
67 *Id.* at 84–85.
68 *Id.* at 85.
69 Creta, *supra* note 42, at 40.
70 *Id.*
71 *Id.*
72 United States v. Cotterman, 709 F.3d 952, 966 (9th Cir. 2013).
73 Creta, *supra* note 42, at 41.

standard itself—"a clear [one] that allows U.S. border agents to detect criminal activity."[74] He says that instead of "changing the legal standard," border patrol agencies' internal control procedures should focus on ways to limit how information obtained from digital devices is shared and stored.[75] Creta contends that the lack of a suspicion-based standard helps maintain national security and makes it easier to prevent terrorism or the spread of child pornography.[76] Creta also argues that this is more practical, since border agents do not have the time to evaluate each case as to whether "there is a reasonable suspicion of criminal activity."[77]

III

Although this issue involves a circuit split, Congress, not the courts, is best suited to resolving this issue.

A. Congress Should Clean Up its Mess

The Supreme Court has acknowledged the border search exception since the nineteenth century.[78] Supreme Court precedent has established the existence of this doctrine,[79] although the limits are disputed today.[80] Nevertheless, the fact remains that this doctrine was instituted by Congress.[81] As such, Congress can modify it as it wishes. Additionally, Congress, unlike the courts, does not need to wait for a lawsuit before changing law; instead, Congress can react more quickly to changing conditions and update any relevant law before the courts have the opportunity to weigh in on an issue.

Gina Bohannon suggests that the courts, not Congress, should establish policy here that protects individuals' privacy interests.[82] She says that the Supreme Court in *Riley* agreed with this assessment.[83] However, the *Riley* court is referring to internal agency protocols as not being ideal here.[84] That does not negate Congress's right and responsibility to fix laws that no longer prove workable. Regardless of the *Riley* court's sentiments, that statement remains dicta. The border search doctrine rests on

---

74 *Id.* at 41–42.

75 *Id.* at 41.

76 *Id.* at 42.

77 *Id.* at 43.

78 *See, e.g.*, United States v. Ramsey, 431 U.S. 606, 617 (1977).

79 *Id.* (citing Boyd v. United States, 116 U.S. 616, 623 (1886)).

80 *See, e.g.*, United States v. Kolsuz, 890 F.3d 133, 144 (4th Cir. 2018); United States v. Cano, 934 F.3d 1002, 1020 (9th Cir. 2019); United States v. Rascon-Ortiz, 994 F.2d 749, 752 n.3 (10th Cir. 1993); United States v. Touset, 890 F.3d 1227, 1233 (11th Cir. 2018).

81 Act of July 31, 1789, ch. 5, §§ 23-24, 1 Stat. 29, 43.

82 *See* Bohannon, *supra* note 42, at 602.

83 *See id.*; Riley v. California, 573 U.S. 373, 398 (2014) ("[T]he Founders did not fight a revolution to gain the right to government agency protocols.").

84 *See Riley*, 573 U.S. at 398.

codified law,[85] and only Congress is constitutionally endowed to change the law.[86]

Indeed, the court system has proven itself incapable of resolving this issue. The four-circuit split shows that regardless of whether a warrant requirement, balancing test, or some other method should be adopted, it will not be uniform across the country. Moreover, the fact that the Supreme Court denied certiorari to a case that could have ultimately resolved this issue[87] implies that the Court either does not feel ready to take a position or does not see a problem with travelers being subjected to different standards depending on where they enter the country.[88]

B. Balancing Tests do not Work

Courts have used balancing tests in a number of cases to attempt to resolve complex issues across the legal spectrum. Examples include the admissibility of certain kinds of evidence,[89] the First Amendment right to free speech,[90] and whether to grant a preliminary injunction.[91] One might argue that the prevalence of balancing tests means that they are a good solution to resolving legal issues with many moving parts and competing interests. However, that is not always the case. Balancing tests inherently involve uncertainty, which makes them impractical for weighing truly important issues.[92]

Additionally, courts often make mistakes when applying balancing tests, or apply them inconsistently, which may require the intervention of a higher court. For example, the balancing test in Federal Rule of Evidence 609(a) "produced confusion among the circuits."[93] Circuit courts were split across three separate issues regarding this test by the time it reached the Eleventh Circuit in *Brown v. Flury*.[94] However, the Eleventh Circuit ultimately refused to make its own decision as to how to apply that balancing test, resolving the case before applying it to the facts.[95]

---

85 Act of July 31, 1789, ch. 5, §§ 23-24, 1 Stat. 29, 43.

86 U.S. CONST. art. I, § 1.

87 *See generally* United States v. Williams, 942 F.3d 1187 (10th Cir. 2019), *cert. denied,* 141 S. Ct. 235 (2020).

88 *See* J. Alexander Lawrence & Sara Stearns, *Uncertainty Around Border Phone Search Continues*, LAW 360 (Nov. 20, 2020), https://www.law360.com/articles/1329867/uncertainty-around-border-phone-search-standardcontinues.

89 *See* Brown v. Flury, 848 F.2d 158, 159 (11th Cir. 1988).

90 *See* Connick v. Myers, 461 U.S. 138, 150 (1983); Pickering v. Bd. of Educ., 391 U.S. 563, 568 (1968).

91 *See* Winter v. Natural Resource Defense Council, Inc., 555 U.S. 7, 24 (2008).

92 *See, e.g.,* Jaffee v. Redmond, 518 U.S. 1, 17–18 (1996) (rejecting *ex post* balancing in determining the applicability of psychotherapist privilege given the difficulty patients and psychotherapists would experience in predicting whether their conversations are privileged).

93 *Brown*, 848 F.2d at 159.

94 *Id.*

95 *Id.*

Similarly, the First Amendment balancing test as laid out in *Pickering v. Board of Education* and *Connick v. Myers* has been subject to misapplication and error by the courts.[96] The Supreme Court in *Connick* attributed clear error to the district court's application of the test in that case.[97] However, the Court also said that "such particularized balancing is difficult" but "courts must reach the most appropriate possible balance of the competing interests."[98] This statement is an admission of the difficulty of applying balancing tests in certain cases, yet somehow courts are expected to reach the most equitable solution each time. Legal scholar Jonathan Alen Marks has criticized the *Connick* court's application of the *Pickering* balance test.[99] He says that this decision, along with similar ones, shows that balancing tests are applied in a "discordant and unpredictable manner."[100] Marks points to specific errors in how the *Connick* court applied the *Pickering* test and contrasts those to how the Court applied the test in other cases.[101] As such, it makes sense to move away from balancing tests in cases involving digital devices and border searches, despite what Caroline McCaffrey argues.[102] Indeed, the multi-factor balancing test that McCaffrey proposes has enough moving parts that a court could easily misapply it.[103]

A later Supreme Court case highlights the difficulties of applying multi-factor balancing tests. In *Winter v. Natural Resource Defense Council, Inc.*, the Court points out that the district court did not properly "asses[ ] the balance of equities and the public interest."[104] Indeed, the Ninth Circuit panel that reviewed the case before it reached the Supreme Court came to the same conclusion.[105] However, the Supreme Court reversed the Ninth Circuit's granting of a preliminary injunction, relying on its own application of the relevant balancing test here.[106] The procedural history of this case illustrates the inherent uncertainty involved in balancing tests and shows why they are not an appropriate solution to complex legal issues.

Instead of a balancing test, any law that Congress would write to resolve the issue of digital devices and border searches should take one of two approaches. It should involve either some sort of reasonable sus-

---

96 *See* Connick v. Myers, 461 U.S. 138, 150 (1983).

97 *Id.* at 149–50.

98 *Id.* at 150.

99 *See* Jonathan Alen Marks, *Connick v. Myers: Narrowing the Scope of Protected Speech for Public Employees*, 5 U. BRIDGEPORT L. REV. 337, 338 (1984).

100 *Id.* at 351–52.

101 *Id.* at 353–57.

102 McCaffrey, *supra* note 42, at 240.

103 *See id.*

104 Winter v. Natural Resources Defense Council, 555 U.S. 7, 26 (2008).

105 *Id.* at 27.

106 *Id.* at 33.

picion standard as articulated by one of the circuit courts (or based on different criteria), or it should clearly delineate a set of circumstances in which border agents are allowed to search digital devices. A reasonable suspicion standard involves vagueness and uncertainty of its own, but it does not need to include a set of factors that are unwieldy and difficult to apply; such standards can be simple, and they can be molded to apply to many situations as needed. Similarly, a list of circumstances also would not be definitive, but it would provide clear guidelines as to when a search is appropriate instead of trying to figure out which nebulous interest is more powerful than another nebulous interest, as would be necessary with a balancing test.

C. Who Needs a Warrant?

The push to establish a search warrant requirement for searching digital devices at the border undermines the purpose of the border search doctrine. Despite Gina Bohannon's assertion that the purpose of the border search doctrine is to keep physical, not digital, contraband out of the United States,[107] there is such a concept as digital contraband. The Ninth Circuit in *United States v. Cano* put it clearly: "The best example is child pornography."[108] Digital devices did not exist when the 1st Congress enacted the border search doctrine, but the concept of contraband has not changed much since then; only the medium has.[109]

Furthermore, the fact that contraband may be digital today does not negate the fact that the United States has a strong interest in preventing it from entering the country. As further stated by the *Cano* court, "[B]ecause cell phones may ultimately be released into the interior . . . the United States has a strong interest in preventing the entry of such material."[110] In light of the fact that digital contraband is an important consideration during border searches, it does not make sense to take the extra step of requiring a search warrant in such cases. Indeed, the Supreme Court has recognized that the government has a strong interest in preventing contraband, in any form, from entering the country. In *United States v. Flores-Montano*, Chief Justice Rehnquist asserted that "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border."[111] Combined with the 1st Congress's decision to explicitly not require a search warrant for

---

107 *See* Bohannon, *supra* 42 at 594–96.

108 United States v. Cano, 934 F.3d 1002, 1014 (9th Cir. 2019).

109 *Compare* SAMUEL JOHNSON, A DICTIONARY OF THE ENGLISH LANGUAGE (5th ed. 1773) (defining contraband as that which is "[p]rohibited; illegal; unlawful") *with Contraband*, BLACK'S LAW DICTIONARY (5th ed. 1979) (defining contraband generally as "any property which is unlawful to produce or possess").

110 *Cano*, 934 F.3d at 1020.

111 U.S. v. Flores-Montano, 541 U.S. 149, 152 (2004).

searches at border crossings, this is a strong argument against calls for the search warrant requirement to be extended to such situations.

Nevertheless, it is true that digital devices contain important and personal information that needs to be protected.[112] The Electronic Frontier Foundation (EFF), a digital privacy rights group, found that as of 2016, border agents were increasing their searches of digital devices.[113] As will be discussed,[114] any law that Congress would pass should include strong privacy protections. However, these protections must be balanced against the need for the government to prevent contraband from entering the country. As such, while a requirement for a search warrant would be too strong, a reasonable suspicion standard would strike the correct balance between protecting people's privacy and protecting the country's national security.

IV

This Note has hopefully established the importance of fine-tuning the border search doctrine regarding digital devices and why it should be Congress, not the courts, that fixes this problem. This section will discuss the relevance of digital privacy today and explain why such protections are important for any statute that Congress might pass to resolve this issue.

A. Why Data Protections are Important

The usage of digital devices has exploded in recent years. Pew Research Center found in 2019 that ninety-six percent of Americans owned a cellphone, with eighty-one percent owning a smartphone.[115] Three billion people worldwide own smartphones, with another several hundred million expected to enter that category over the next few years.[116] Pew also found that almost seventy-five percent of Americans own other digital devices, such as laptops.[117] These numbers have important ramifications when it comes to the ability of border agents to search people's digital devices. Specifically, international travel between the United

---

112 *See, e.g.,* Bohannon, *supra* note 42, at 566 ("Even just ten years ago, lawmakers and judges perhaps did not contemplate the excessive amounts of personal data now found in small rectangular devices . . . nearly half of all Americans say they could not live without.").

113 SOPHIA COPE, AMUL KALIA, SETH SCHOEN, & ADAM SCHWARTZ, DIGITAL PRIVACY AT THE U.S. BORDER: PROTECTING THE DATA ON YOUR DEVICES, ELECTRONIC FRONTIER FOUNDATION 5 (2017), https://www.eff.org/files/2018/01/11/digital-privacy-border-12-2017.pdf.

114 *See infra* Part IV.

115 *Mobile Fact Sheet*, PEW RES. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/.

116 S. O'Dea, *Smartphone Users Worldwide 2016-2026*, STATISTA (Mar. 31, 2021), https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/.

117 *Mobile Fact Sheet*, *supra* note 115.

States and other countries in 2019 increased by 2.4 percent from 2018, with a total of 241 million passengers traveling through a United States airport.[118] As the EFF found, since United States border agents are increasing their searches of digital devices,[119] it is important for Congress to enact safeguards to protect people's data and privacy.

Besides for the sheer prevalence of digital devices, people also use them to store sensitive and private information. Laptops, for example, can keep records of someone's passwords, which might enable border agents to access that person's email or bank accounts.[120] Smartphones commonly store photos.[121] Those might not be inherently sensitive, but they are undoubtedly personal, and many people may feel uncomfortable if border agents were able to wantonly examine them. The Federal Trade Commission recommends that people take basic protections for their phones, such as setting a passcode, precisely because phones contain sensitive and personal information.[122] Police officers have been documented abusing access to confidential information,[123] so it is important to have strong protections in place to prevent this from happening in other cases, particularly when travelers already have decreased privacy rights at border crossings.

B. What Protections Should Congress Include in a Potential Bill?

As discussed earlier in this Note, Congress should either enact a reasonable suspicion standard or create a list of circumstances under which it is acceptable to conduct a search.[124] Along with that, Congress should also ensure that border agents properly access and store the data from any digital device, as well as provide documentation and details of each search.

---

118 Press Release, 2019 Traffic Data for U.S. Airlines and Foreign Airlines U.S. Flights – Final, Full-Year, Bureau of Transportation Statistics (Mar. 19, 2020), https://www.bts.gov/newsroom/final-full-year-2019-traffic-data-us-airlines-and-foreign-airlines.

119 COPE ET AL., *supra* note 113, at 5.

120 *See* Whitson Gordon, *The One Thing that Protects a Laptop After it's Been Stolen*, N.Y. TIMES (Mar. 13, 2018), https://www.nytimes.com/2018/03/13/smarter-living/how-to-encrypt-your-computers-data.html.

121 *See* Erik Sofge, *What Personal Data Stays on a Phone?*, CONSUMER REPORTS (Mar. 23, 2016), https://www.consmerreports.org/cell-phones-services/what-personal-data-stays-on-your-phone-/.

122 *How to Protect Your Phone and the Data on It*, FED. TRADE COMM'N. (Sept. 2019), https://www.consumer.ftc.gov/articles/how-to-protect-your-phone-and-data-it.

123 Sadie Gurman, *AP: Across the U.S., Police Officers Abuse Confidential Databases*, ASSOCIATED PRESS (Sept.28, 2016), https://apnews.com/article/699236946e314065fff8a2362e16f43?utm_campaign=socialFlow&utm_source=Twitter&utm_medium=AP.

124 *See supra* Part III.B; *supra* Part III.C.

1. Accessing the Data

For any search, Congress should clearly indicate who has permission to conduct the search. Congress may wish to differentiate between a basic search and a forensic search.[125] Border agents may be allowed to conduct a basic search at the airport, but only certain agencies may be allowed to conduct forensic searches. Congress should also create, or authorize the relevant agencies to create, procedures for how to access the data in order to prevent damage to the device or corruption of the data.[126] Such procedures should be updated as frequently as necessary to take advantage of changing technology. Such procedures, if they require specific software, should also be continuously monitored to ensure that the procedures and software involved do not damage people's devices.

When conducting basic searches, it would make sense to codify an allowance for the person whose device is being searched to be present, and allowed to observe, during the search.[127] This would prevent miscommunication about what the search was intended to uncover and would make any subsequent criminal investigation proceed more smoothly. To that end, all searches should be documented in writing, including why the device is being searched, what the search is intended to uncover, and who was present and who conducted the search.[128] Similarly, any searches, basic or forensic, should be conducted with more than one agent present, to provide additional descriptions of what occurred and what was found.[129] Agents should be trained in proper search procedures and only properly trained agents should be allowed to conduct searches. This would lessen the chance of irreparable harm occurring, either to the device or to potential evidence, if someone without the requisite skills attempts to conduct the search.

Some of these proposed protections are mentioned in a report by DHS.[130] Specifically, the report discusses who can search the devices

---

125 *See* United States v. Kolsuz, 890 F.3d 133, 138 (4th Cir. 2018) (discussing "nonroutine" border searches); United States v. Cano, 934 F.3d 1002, 1020 (9th Cir. 2019) (discussing circumstances under which border officials can conduct forensic searches); United States v. Touset, 890 F.3d 1227, 1233–34 (11th Cir. 2018) (holding that forensic searches are no different from regular searches of property).

126 See McCaffrey, *supra* note 42, at 241–44, for a discussion of some of the issues involved in current border search procedures and how a multi-factor balancing test might resolve them. But see *supra* Part III.B for a discussion of why a balancing test would ultimately not accomplish this goal.

127 *Id.*

128 *See id.* at 241.

129 *See id.* at 242.

130 *See generally* DEP'T HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE U.S. BORDER PATROL DIGITAL FORENSICS PROGRAMS, DEP'T HOMELAND SECURITY (July 30, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp053a-digitalforensics-july2020.pdf [hereinafter PRIVACY IMPACT ASSESSMENT].

and how to provide notice to individuals that CBP is going to search their devices.[131] However, these protections, in their current form, are weak. They rely on the goodwill of CBP not to change their procedures, not on any overarching law. Furthermore, the channels that CBP uses to provide notice are particularly inefficient. The report says that CBP will conduct searches in the presence of the affected individual "when possible," except in cases of "national security, law enforcement, officer safety, or other operational considerations."[132] Those terms are not defined and leave much room for interpretation. Additionally, the report says that even if the individual can be present for the search, they might not be allowed to "observe the search" if "the search could reveal law enforcement techniques or potentially compromise operations."[133] This is a large loophole that could potentially allow CBP to violate someone's privacy without the individual being aware. Clear guidelines, codified into law, would prevent this. Finally, CBP relies on a report published in 2018 as notice that they can search digital devices.[134] However, how is that supposed to provide effective notice if people are not aware of the report? It is unlikely that many travelers take the time to scour the CBP or DHS websites for possibly obscure reports about situations that they might not have considered prior to traveling and being stopped.

The Supreme Court might prefer that administrative agencies not create solutions to this problem.[135] However, the Court would arguably have less of an objection if Congress explicitly charged the agencies with creating solutions in the way of internal procedures, or even codified the procedures directly. The Court's objections to government procedures in *Riley* did not disparage government procedures entirely.[136] In that case, the Court was concerned about vague and inconsistent procedures across different situations,[137] which would not apply here if Congress were to clarify a proper approach in the first place.

2. Storing the Data

Besides for how border agents access the data, Congress should enact protections for how, how long, and where that data is stored. CBP currently stores information obtained from digital devices for 20 years if the data "does not lead to an individual's arrest, detention, or re-

131 *Id.* at 8.

132 *Id.*

133 *Id.*

134 *Id.* at 7; *see generally* DEP'T HOMELAND SEC., CBP BORDER SEARCHES OF ELECTRONIC DEVICES (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.

135 *See* Riley v. California, 573 U.S. 373, 398 (2014).

136 *Id.*

137 *See id.* at 391.

moval."[138] If the individual was arrested, detained, or removed, CBP might store the data for 75 years.[139] CBP does not indicate how that data is protected while in CBP's possession.[140] Indeed, CBP does not indicate whether the data remains in CBP's possession at all,[141] although an earlier report attempts to describe when CBP will share this data.[142]

Arguably, there are very few cases where CBP would legitimately need to retain this data for so long. Instead, Congress should codify time limits after which CBP must delete the data. For example, if a search does not result in the arrest, detention, or removal of the person, the data should be deleted immediately, since CBP would have no further need for it. If a search results in someone's arrest, detention, or removal, CBP should delete the data when the criminal procedure ends, including any appeals. The only exceptions should be in cases of legitimate national security, as defined by Congress, not CBP.

Additionally, Congress should require CBP to store the data securely and ensure that there is no inadvertent harm to someone's privacy, even if CBP must share that data with other agencies. CBP's current response to privacy concerns is telling: "This risk is mitigated because CBP notifies record recipients that it must not share the information with third parties without prior CBP approval."[143] This is the equivalent of expecting someone not to do something simply because you tell them not to. The entirety of CBP's procedures regarding the search, storage, and usage of data obtained from digital devices appears to rest on the agency's goodwill, which increases the potential for abuse.

CONCLUSION

Congress should pass a law requiring either a reasonable suspicion standard for forensic searches of electronic devices at the border, or otherwise create a list of circumstances under which it is reasonable for border agents to search people's electronic devices. Regardless of the approach, the law should include strong protections for the privacy of any information obtained from such searches, including the use, retention, and sharing of any such data.

This approach strikes a middle ground between no standard, as articulated by the Eleventh Circuit,[144] and a full-fledged search warrant

138 PRIVACY IMPACT ASSESSMENT, *supra* note 131, at 8.

139 *Id.*

140 *See id.*

141 *Id.*

142 DEP'T HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE U.S. BORDER PATROL DIGITAL FORENSICS PROGRAMS 15 (Apr. 6, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp053-digitalforensics-april2018.pdf.

143 *Id.*

144 United States v. Touset, 890 F.3d 1227, 1233 (11th Cir. 2018).

requirement, as proposed by some legal scholars and politicians.[145] It resolves the confusion that is inherent when four Circuit Courts of Appeal reach different conclusions on the same issue.[146] It also unifies the approach of the three circuit courts that would implement a reasonable suspicion standard.[147] The job of unification would normally fall to the Supreme Court, but the Court has decided to abstain from this issue, leaving it to Congress to resolve.[148] Nevertheless, as discussed in this Note,[149] it is Congress, not the Supreme Court, that should fix this problem in the first place.

Whichever approach Congress might take to resolve this issue, there is a chance that it would be struck down as unconstitutional. In that case, there is a chance that this issue would remain as splintered and unresolved as it is currently. If a circuit court strikes down the proposed statute, that would leave the legal status of this issue as murky as it is now, with different circuit courts taking different positions. On the other hand, if the Supreme Court is the one to strike down the statute, that could provide clarity on this issue, as hopefully the Court would articulate which aspects of the statute were problematic. As this proposed statute would incorporate elements of the reasoning from the Fourth, Ninth, and Tenth Circuits' decisions, that could require the relevant circuit(s) to approach this issue differently, and might result in a uniform solution. Additionally, as a new statute would almost inevitably result in litigation, that could force the Supreme Court to finally resolve this issue, especially since this issue does not appear likely to vanish anytime soon. Although the Court refused to hear a recent case on this issue, if more cases wind their way through the court system, it might have no choice but to weigh in. In such a case, even if the legislation proposed in this Note is not immediately effective in resolving the current issue, it might yet have an impact by requiring the Supreme Court to make a decision anyway.

---

145 Bohannon, *supra* note 42, at 603.

146 *See* United States v. Kolsuz, 890 F.3d 133, 144 (4th Cir. 2018); United States v. Cano, 934 F.3d 1002, 1020 (9th Cir. 2019); United States v. Rascon-Ortiz, 994 F.2d 749, 752 n.3 (10th Cir. 1993); United States v. Touset, 890 F.3d 1227, 1233 (11th Cir. 2018).

147 *See Kolsuz*, 890 F.3d at 144; *Cano*, 934 F.3d at 1020; *Rascon-Ortiz*, 994 F.2d at 752 n.3.

148 *See generally* United States v. Williams, 942 F.3d 1187 (10th Cir. 2019), *cert. denied,* 141 S. Ct. 235 (2020).

149 *See supra* Part III.A.