Michigan Law Review

Volume 118 | Issue 3 Article 5

2019

Forensic Border Searches After *Carpenter* Require Probable Cause and a Warrant

Christopher I. Pryby
University of Michigan Law School

https://doi.org/10.36644/mlr.118.3.forensic

NOTE

FORENSIC BORDER SEARCHES AFTER *CARPENTER* REQUIRE PROBABLE CAUSE AND A WARRANT

*Christopher I. Pryby**

Under the border search doctrine, courts have upheld the federal government's practice of searching people and their possessions upon entry into or exit from the United States, without any requirement of suspicion, as reasonable under the Fourth Amendment. Since the advent of electronic devices with large storage capacities, courts have grappled with whether this definition of reasonableness continues to apply. So far, courts have consistently characterized "nonforensic" border inspections of electronic devices (for example, paging through photos on a phone) as "routine" searches that, like inspecting luggage brought across international lines, require no suspicion. But there is a circuit split over what suspicion the government needs to conduct "forensic" searches that copy data for later inspection. This Note argues that the recent Supreme Court decision in Carpenter v. United States *recognized a new balance of privacy rights at the border. Starting in* United States v. Jones *and continuing through* Riley v. California *and* Carpenter*, the Court has developed a theory of data privacy aimed at forestalling the government's creation of a high-tech panopticon. This new theory, in the context of electronic searches at the border, requires that the balance of government and individual interests be struck in favor of the individual. Probable cause and a warrant, not merely reasonable suspicion, are necessary for a forensic search.*

TABLE OF CONTENTS

---

* J.D. Candidate, May 2020, University of Michigan Law School. I would like to thank Professor Evan Caminker for his insights on *Carpenter* and his thoughtful feedback on this Note. I am grateful to Professors Barbara McQuade and Eve Brensike Primus for discussions about the impact of *Riley* and *Carpenter* on the border search doctrine. I also thank Shaughn Casey, Kellie Majcher, James Williams, Matthew Williams, and Daniel Winston-Ruiz for enlightening conversations, not to mention all the attendees of Michigan Law's Student Research Roundtable for their helpful questions and comments.

INTRODUCTION

Pascal, a dual citizen of the United States and France, is a doctoral student in Islamic studies at a Canadian university. He is riding an Amtrak train from Montreal to New York when Customs and Border Protection (CBP) agents board the train at the U.S.-Canada border. During questioning, Pascal admits that he has lived in Jordan and visited Lebanon in the past year. The agents order him to bring his luggage to the dining car for inspection and to unlock his laptop. While inspecting files on his computer, they see images of Hezbollah and Hamas rallies. Unsatisfied with Pascal's explanation that he observed the rallies as research for his dissertation, the agents confiscate his laptop and other electronics for further search. The agents release him later that day and return his cell phones and camera, but they send his laptop and external hard drive to Immigration and Customs Enforcement (ICE). Pascal receives those items by mail eleven days later. He is never charged with a crime, but it is clear that, at a minimum, agents have viewed files including personal photographs, messages with his girlfriend, and emails. It is possible they logged into his social networking accounts too. He further suspects that ICE has retained copies of the data from his devices.

This is not a contrived hypothetical. The facts above come from a real case: *Abidor v. Napolitano*.[1] Travelers are accustomed to certain invasions of physical privacy as part of the norms of the exercise—it is the price of keeping would-be terrorists off planes. For international travelers, a customs inspection is also possible—and about as welcome as a jury summons. But many Americans do not realize the extent to which the government asserts

1. 990 F. Supp. 2d 260 (E.D.N.Y. 2013).

authority to inspect anything entering or leaving the country.[2] The border search doctrine has traditionally required no suspicion at all for government agents to search anything at the border,[3] and courts have only recently begun to consider whether this ability to search "anything" should include the contents of travelers' phones, cameras, and laptops.

This issue deserves close scrutiny. First, troublingly expansive interpretations of the border search doctrine are not confined to a single political party or ideology. In fact, although generally considered friendlier to civil rights than the Trump Administration,[4] the Obama Administration claimed the power to conduct the search at issue in *Abidor*. Second, there is a circuit split on the issue. Although federal courts of appeals have unanimously held that no suspicion is needed if agents merely look at files on electronic devices at the border, they are divided on whether agents need some amount of suspicion to copy the contents of those devices for later review (a "forensic search"). Third, a recent line of Supreme Court cases on Fourth Amendment rights, most recently *Carpenter v. United States*,[5] has endorsed reasoning that compels a reexamination of the border search doctrine's applicability to electronic data.

This Note argues that reasonable suspicion is not enough. Specifically, courts should require the government to develop probable cause that a device contains evidence of a crime before it conducts a forensic border search on that device. Part I reviews the border search doctrine's history and its traditional bifurcation between "routine" and "nonroutine" searches. Part II examines how the doctrine has come into conflict with separate precedent governing electronic data privacy. In particular, it explores the circuit split—between the Fourth and Ninth Circuits on the one hand and the Eleventh Circuit on the other—and these courts' attempts to reconcile the historical border search exception with recent Supreme Court decisions. Finally, Part III contends that the balance of government and individual interests, viewed through the lens of Supreme Court data privacy precedent, requires probable cause and a warrant for a forensic border search.

---

2. *E.g.*, Patrick G. Lee, *Can Customs and Border Officials Search Your Phone? These Are Your Rights*, PROPUBLICA (Mar. 13, 2017, 12:55 PM), https://www.propublica.org/article/can-customs-border-protection-search-phone-legal-rights [https://perma.cc/37J7-85TY] ("The unsettling fact is that border officials have long had broad powers—many people just don't know about them.").

3. *See infra* Part I.

4. *See, e.g.*, *Trump Administration Civil and Human Rights Rollbacks*, LEADERSHIP CONF. ON CIV. & HUM. RTS., https://civilrights.org/trump-rollbacks [https://perma.cc/H22Y-UZME] (collecting actions by the Trump Administration alleged to infringe on civil rights, including rollbacks of some Obama Administration policies).

5. 138 S. Ct. 2206 (2018).

I. THE BORDER SEARCH EXCEPTION

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects[] against unreasonable searches and seizures."[6] But unlike searches in the interior of the country, border searches have never required probable cause.[7] This Part describes the origins and traditional operation of the border search doctrine. Section I.A focuses on three primary justifications for suspicionless border searches: the history of the practice, original understandings of what constitutes a reasonable search, and the balance of government and individual interests. Section I.B discusses the distinction between routine and nonroutine border searches and the level of suspicion courts have required for each.

A. *Doctrinal Origins*

The border search exception to the general warrant and probable cause requirements "has a history as old as the Fourth Amendment itself."[8] The Constitution grants Congress "broad, comprehensive powers '[t]o regulate Commerce with foreign Nations,'"[9] including the ability to exclude aliens and property and to interdict smuggling.[10] In fact, from the Founding, customs officials routinely inspected imports to assess duties and seize contraband.[11] And the Supreme Court has recognized a "longstanding right of the sovereign to protect itself" by inspecting persons and items entering the country.[12] Moreover, the Court has stressed that the border search exception does not result from "exigent circumstances," like some exceptions to the warrant requirement, but is instead founded on a "historically recognized exception" to the warrant requirement, much like the rule permitting a search incident to a lawful arrest.[13]

The Court has also marshalled an original-understanding argument to justify the border search exception. The first Congress, the same that drafted the Bill of Rights, enacted a law authorizing customs officials "on suspicion of fraud, to open and examine . . . any package or packages" and to board

---

6. U.S. CONST. amend. IV.

7. United States v. Ramsey, 431 U.S. 606, 619 (1977).

8. *Id.*

9. United States v. Twelve 200-Ft. Reels of Super 8mm Film, 413 U.S. 123, 125 (1973) (alteration in original) (quoting U.S. CONST. art. I, § 8, cl. 3).

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

11. *See id.* at 616, 619; United States v. Thirty-Seven (37) Photographs, 402 U.S. 363, 376 (1971) (describing customs inspections as "an old practice . . . intimately associated with excluding illegal articles from the country").

12. *Ramsey*, 431 U.S. at 616; *see also* United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985) ("Since the founding of our Republic, 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.").

13. *Ramsey*, 431 U.S. at 621. For searches incident to lawful arrest, see *infra* note 62.

and search "any ship or vessel[] in which they shall have reason to suspect any goods . . . subject to duty shall be concealed" and seize any contraband found.[14] Because that same Congress drafted the Fourth Amendment, the Court has inferred that "reasonable searches and seizures" must encompass the border searches authorized in that statute. Therefore, says the Court, modern-day border searches are likewise reasonable.[15]

Besides looking to historical understandings of reasonableness, the Court also determines whether a category of searches is reasonable by "balancing the [government's] need to search against the [personal] invasion which the search entails."[16] This kind of interest balancing justifies the border search exception. The Court has consistently recognized that "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border"[17]—this interest is so powerful that border searches "are reasonable simply by virtue of the fact that they occur at the border."[18] Additionally, the Court has held that individuals generally enjoy a diminished expectation of privacy in such circumstances.[19]

B. *Classifications of Border Searches*

The border search exception to the probable cause and warrant requirements is firmly entrenched in Fourth Amendment doctrine.[20] Yet there

---

14. Act of July 31, 1789, ch. 5, §§ 23–24, 1 Stat. 29, 43, *repealed and replaced by* Act of Aug. 4, 1790, ch. 35, §§ 47–48, 1 Stat. 145, 169–70 (containing the same language).

15. *Ramsey*, 431 U.S. at 616–17, 619; Boyd v. United States, 116 U.S. 616, 623 (1886). But *Boyd* and *Ramsey* misread the extent of the statutes. Far from permitting customs inspectors to search cargo without "*any* level of suspicion," Recent Case, United States v. Touset*: Eleventh Circuit Holds That Border Searches of Property Require No Suspicion*, 132 HARV. L. REV. 1112, 1116 (2019), the latter act only permitted inspectors to board a ship and take account of and affix seals to "any box, trunk, chest, cask, or other package . . . separate from . . . the cargo," Act of Aug. 4, 1790, ch. 35, § 31, 1 Stat. at 164–65. This language does not prove "that the First Congress did not understand the Fourth Amendment to require individualized suspicion to search property at the border," Recent Case, *supra* at 1116. Although the second act did permit inspectors to search the entirety of a vessel *for* cargo, it did not authorize inspectors to search the cargo itself. Thus, the act is better read as retaining a suspicion requirement before permitting plenary searches of personal property.

16. Camara v. Mun. Court of S.F., 387 U.S. 523, 537 (1967).

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

18. *Ramsey*, 431 U.S. at 616; *see also* United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985) ("[T]he Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior.").

19. *See, e.g.*, *Montoya de Hernandez*, 473 U.S. at 538 n.1 ("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." (quoting Carroll v. United States, 267 U.S. 132, 154 (1925))).

20. *But see* United States v. Vergara, 884 F.3d 1309, 1313 (11th Cir. 2018) (J. Pryor, J., dissenting) ("[I]n my view, a forensic search of a cell phone at the border requires a warrant supported by probable cause.").

are still constitutional limits on searches at the border. This Section will examine two categories of traditional, nonelectronic border searches—routine and nonroutine searches—and the requirements courts have imposed on them.

In general, "[r]outine searches of the persons and effects of entrants" into the country "are not subject to any requirement of reasonable suspicion, probable cause, or warrant."[21] Routine searches include the kinds of inspections an average international traveler is acquainted with: looking through luggage, checking vehicles for drugs, and conducting pat-downs and frisks.[22] Still more intrusive searches are considered routine and have no suspicion requirement, including opening and inspecting international mail[23] and even removing and disassembling a car's gas tank.[24]

But not all such searches are routine. The Supreme Court in *United States v. Ramsey* first hinted that a border search might be " 'unreasonable' because of the particularly offensive manner in which it is carried out."[25] Yet it was not until *United States v. Montoya de Hernandez* that the Court first ruled on that issue.[26] There, the Court held that the "reasonable suspicion" standard—a lower standard than probable cause—under which "officials at the border must have a 'particularized and objective basis for suspecting [a] particular person,' " applied to border crossers suspected of smuggling drugs in their bodies.[27] The Court found that the reasonable suspicion standard fit well because that "type of smuggling gives no external signs and inspectors will rarely possess probable cause to arrest or search" and the government's interest in stopping drug smuggling remains high.[28] The *Montoya de Hernandez* Court further held that the scope of the intrusion—here, including incommunicado detention without a court order for nearly a full day and an alternative between either defecating into a wastebasket under the "watchful eyes of two attending matrons" or submitting to an abdominal x-ray while handcuffed[29]—was justified by the reasonable suspicion standard.[30]

Perhaps because of how intrusive the *Montoya de Hernandez* search was, lower courts have taken the case to require reasonable suspicion only for in-

21. *Montoya de Hernandez*, 473 U.S. at 538.

22. *See* United States v. Saboonchi, 990 F. Supp. 2d 536, 549 (D. Md. 2014).

23. *See Ramsey*, 431 U.S. at 619–20. The informational content of the letters, however, was protected by regulation. *Id.* at 623.

24. United States v. Flores-Montano, 541 U.S. 149, 155 (2004). However, the Court noted that the search did not irreversibly destroy the gas tank and that the outcome might have differed if it had. *Id.* at 155–56.

25. 431 U.S. at 618 n.13.

26. 473 U.S. at 540 ("We have not previously decided what level of suspicion would justify a seizure of an incoming traveler for purposes other than a routine border search.").

27. *Montoya de Hernandez*, 473 U.S. at 541–42 (quoting United States v. Cortez, 449 U.S. 411, 417 (1981)).

28. *Id.*

29. *Id.* at 546–47 (Brennan, J., dissenting).

30. *Id.* at 542–44 (majority opinion).

vasive border searches like strip searches and body cavity searches.[31] Indeed, the Court appeared to affirm this understanding in *United States v. Flores-Montano*, explaining that the reasons supporting a suspicion requirement in "highly intrusive searches of the person—dignity and privacy interests of the person being searched—simply do not carry over to vehicles."[32] Some lower courts have even held that only searches of the person, not of property, require any level of suspicion at all, reading *Flores-Montano* to reject any distinction between "routine" and "nonroutine" searches.[33] Still other courts have attempted to articulate factors distinguishing the two.[34] And the Supreme Court has not yet foreclosed the possibility that certain property searches could be "'so destructive,' 'particularly offensive,' or overly intrusive in the manner in which they are carried out" that at least some suspicion is necessary.[35] In sum, however, once a court classifies a border search as routine or nonroutine, that classification determines the level of suspicion the government needs.

II. ELECTRONIC PRIVACY AND CONFLICT WITH THE BORDER SEARCH EXCEPTION

So far, this Note has limited its discussion to traditional searches of persons and property. But the factors relevant to distinguishing between routine and nonroutine searches have become increasingly complicated when applied to new technology. This Part examines how courts have applied the border search exception to data contained in electronic devices. Section II.A discusses the emerging distinction between nonforensic searches and forensic searches. Section II.B then highlights *Carpenter v. United States*, in which the Supreme Court recognized strong Fourth Amendment protections of individuals' right to privacy in their data. Section II.C concludes by exploring the circuit conflict that developed as the lower courts grappled with reconciling the Court's digital privacy doctrine with the longstanding border search doctrine.

---

31. *See, e.g.*, United States v. Braks, 842 F.2d 509, 512–13 (1st Cir. 1988).

32. 541 U.S. 149, 152 (2004).

33. *E.g.*, United States v. Touset, 890 F.3d 1227, 1233 (11th Cir. 2018) ("We have been similarly unwilling to distinguish between different kinds of property. For example, we have upheld 'a search without reasonable suspicion of a crew member's living quarters on a foreign cargo vessel that [wa]s entering this country,' even though '[a] cabin is a crew member's home—and a home "receives the greatest Fourth Amendment protection."'" (alterations in original) (citation omitted) (quoting United States v. Alfaro-Moncada, 607 F.3d 720, 727, 729 (11th Cir. 2010))).

34. For example, the *Braks* court considered factors associated with the suspect's personal dignity and bodily integrity. *Braks*, 842 F.2d at 511–12; *accord* United States v. Vega-Barvo, 729 F.2d 1341, 1346 (11th Cir. 1984). By contrast, the court in *United States v. Saboonchi*, 990 F. Supp. 2d 536, 564 (D. Md. 2014), considered factors related to the amount of information the government can obtain about the suspect.

35. United States v. Cotterman, 709 F.3d 952, 963 (9th Cir. 2013) (en banc) (quoting *Flores-Montano*, 541 U.S. at 152, 154 n.2, 156).

A. *Applying the Doctrine to Electronic Devices*

In applying the border search doctrine to electronic data, courts have attempted to mirror the existing, if not entirely clear, distinction between routine and nonroutine searches. The principal split focuses on the treatment of "nonforensic" and "forensic" searches. The general rule is that a nonforensic search is a search of electronic media limited in duration and scope by the fact that an officer must manually conduct it.[36] For example, if a border agent looks at videos on a camera in a van crossing the border[37] or selects an international airline passenger at random and looks at photos on the passenger's computer,[38] the agent has conducted a nonforensic search. Even searching files on an external hard drive at a customs checkpoint or inspecting a computer's directory tree with the computer's own search functions is nonforensic so long as it remains bound by a human agent's limited time and ability to perform the search in person.[39]

Courts have consistently held that nonforensic searches at the border require no suspicion.[40] Some courts have justified this permissiveness by analogy to routine searches of personal property at the border—just as a border agent needs no suspicion to look inside luggage, she does not need it to look inside a cell phone or a laptop.[41] Moreover, the time and resource constraints on CBP mean that an agent would hardly be in a position to rifle through every personal file of every traveler lumbering past her booth.[42] The intrusion on privacy therefore remains limited in practice despite being unlimited in theory.

---

36. *See* Abidor v. Napolitano, 990 F. Supp. 2d 260, 269–70 (E.D.N.Y. 2013) ("A quick look entails only a cursory search that an officer may perform manually. It involves opening the computer and viewing the computer's contents as any lay person might be capable of doing simply by clicking through various folders.").

37. United States v. Ickes, 393 F.3d 501, 502 (4th Cir. 2005).

38. United States v. Arnold, 533 F.3d 1003, 1005 (9th Cir. 2008).

39. *See Saboonchi*, 990 F. Supp. 2d at 568 ("A conventional computer search allows Customs officers to choose, within the finite amount of time available to them while they detain the traveler, to decide where . . . to focus their attention . . . . A forensic search, on the other hand, allows a Customs officer to give uniquely probing review not only to the files on one's computer, but also any files that ever may have been on that computer. And even after a traveler is cleared to enter the country, the search may continue for months or even years afterwards.").

But new technologies could recognize potentially illegal data on a device more quickly. *See, e.g.*, Mohamed N. Moustafa, Applying Deep Learning to Classify Pornographic Images and Videos (Nov. 28, 2015), https://arxiv.org/pdf/1511.08899.pdf [https://perma.cc/358M-8D9E]. It is doubtful that a time bound will remain a useful heuristic to categorize forensic and nonforensic searches.

40. *See, e.g.*, United States v. Kolsuz, 890 F.3d 133, 140 (4th Cir. 2018) (reporting the district court's holding on this issue); *Arnold*, 533 F.3d at 1008; *Ickes*, 393 F.3d at 502.

41. *See, e.g.*, *Arnold*, 533 F.3d at 1009 ("Arnold has failed to distinguish how the search of his laptop and its electronic contents is logically any different from the suspicionless border searches of travelers' luggage that the Supreme Court and we have allowed.").

42. *Saboonchi*, 990 F. Supp. 2d at 564.

Forensic searches, by contrast, eliminate the inherent time and resource bounds on electronic searches conducted by hand. A forensic search is "an exhaustive search of a computer's entire hard drive"[43] in which the government copies the data stored on a device for later inspection.[44] A forensic search can also access data the user has supposedly deleted—for example, data "emptied from the operating system's trash or recycling bin folder" that the user cannot see or access without using special software.[45]

The Ninth Circuit in *United States v. Cotterman* was the first federal appellate court to decide whether a forensic search of an electronic device at the border requires some amount of suspicion.[46] After an en banc hearing, the court held that reasonable suspicion was required.[47] In *Cotterman*, the government seized the defendant's laptop at the U.S.-Mexico border, copied the contents of its hard drive, and examined that data over the course of months.[48] The Ninth Circuit rejected the government's argument that *Flores-Montano* controlled, distinguishing "[t]he private information individuals store on digital devices" at issue in *Cotterman* from a gas tank's "generic and impersonal contents."[49]

Cotterman came shortly after *United States v. Jones*, in which four justices held that sufficiently long-term warrantless GPS tracking of a suspect's vehicle was a violation of a reasonable expectation of privacy.[50] Additionally, in a concurrence, Justice Sotomayor strongly suggested that surveillance creating "precise, comprehensive record[s] . . . reflect[ing] a wealth of detail" about a person's "familial, political, professional, religious, and sexual associations" that can be "store[d] . . . and efficiently mine[d] . . . years into the future" is similarly unreasonable without a warrant.[51] In line with Justice Sotomayor's concurrence in *Jones*, the Ninth Circuit in *Cotterman* paid "particular heed to the nature of the electronic devices and the attendant expectation of privacy" and compared the procedure to "a computer strip search."[52] The *Cotterman* court emphasized the volume of information electronic de-

43. Abidor v. Napolitano, 990 F. Supp. 2d 260, 270 (E.D.N.Y. 2013).

44. *See, e.g.*, United States v. Cotterman, 709 F.3d 952, 958 (9th Cir. 2013) (en banc) (describing the process by which a computer forensic examiner "cop[ied] the hard drives of [defendant's] electronic devices" and "used forensic software that often must run for several hours to examine" those copies).

45. United States v. Flyer, 633 F.3d 911, 918 (9th Cir. 2011).

46. 709 F.3d at 956–57.

47. *Cotterman*, 709 F.3d at 957.

48. *Id.* at 957–59. The examination included inspecting supposedly deleted files as well as unlocking password-protected files. *Id.*

49. *Id.* at 964.

50. 565 U.S. 400, 431 (2012) (Alito, J., concurring in the judgment).

51. *Jones*, 565 U.S. at 415–16 (Sotomayor, J., concurring).

52. *Cotterman*, 709 F.3d at 964, 966.

vices can store[53] and the "Founders' deep concern with safeguarding the privacy of thoughts and ideas . . . from invasion by the government."[54] Because these devices "often retain sensitive and confidential information" long after their users believe that information to be deleted, the court further expressed concern that travelers could not "make meaningful decisions" about what content to expose to potential search at the border.[55] Given these factors, the forensic search of the defendant's data was "[s]uch a thorough and detailed search of the most intimate details of [his] life" that it substantially intruded on his dignity and privacy interests and was unreasonable under the Fourth Amendment.[56]

The Ninth Circuit balanced the government's "important security concerns" at the border with the "potential unfettered dragnet effect" that might result should the government ever have "the time or resources to seize and search the millions of devices that accompany the millions of travelers" crossing the country's borders.[57] In its view, requiring reasonable suspicion would "leave[] ample room for agents . . . to pick up on subtle cues that criminal activity may be afoot,"[58] and, "[a]s a practical matter, border agents are too busy to do extensive searches . . . unless they have suspicion."[59] The court then adopted reasonable suspicion as the prerequisite for the government to perform a forensic search of an electronic device at the border.[60]

B. *Digital Privacy Trumps a Longstanding Warrant Exception*

The Supreme Court largely confirmed the Ninth Circuit's understanding of electronic privacy about a year later. In *Riley v. California*, the Court found that a warrant was required to search the contents of a cell phone on the arrestee's person[61] despite the longstanding exception permitting a search of an arrestee incident to a lawful arrest.[62] The Court explained that the traditional rationale for the exception—preventing "harm to officers and destruction of evidence"—is inapplicable to electronic data.[63] Cell phone da-

53. *Id.* at 964 (contrasting the "warehouses full of information" modern devices can store with the amount "traditionally circumscribed by the size of [a] traveler's luggage or automobile").

54. *Id.* (internal quotation marks omitted) (quoting United States v. Seljan, 547 F.3d 993, 1014 (9th Cir. 2008) (Kozinski, J., dissenting)).

55. *Id.* at 965.

56. *Id.* at 968.

57. *Id.* at 966.

58. *Id.* at 967 (citing United States v. Tiong, 224 F.3d 1136, 1140 (9th Cir. 2000)).

59. *Id.* at 967 n.14 (quoting United States v. Chaudhry, 424 F.3d 1051, 1054 (9th Cir. 2005) (B. Fletcher, J., concurring)).

60. *Id.* at 968.

61. 573 U.S. 373, 386 (2014).

62. *E.g.*, Weeks v. United States, 232 U.S. 383, 392 (1914) (establishing the exception).

63. *Riley*, 573 U.S. at 385–86 ("Absent more precise guidance from the founding era, we generally determine whether to exempt a given type of search from the warrant requirement

ta itself is not a weapon, nor is there "any risk that the arrestee himself will be able to delete incriminating data from the phone" once police have secured it while they wait for a warrant.[64]

Riley also highlighted that an arrestee's privacy interests, albeit "diminished," may still be "weighty enough" to require a warrant.[65] Recalling the "top-to-bottom search of a man's house" of *Chimel v. California*, the Court noted that searching a phone "would typically expose to the government far *more* than the most exhaustive search of a house."[66] Just as the Ninth Circuit did in *Cotterman*, the Court pointed to cell phones' "immense storage capacity" and the intimacy of their contents as causes for concern about indiscriminate phone searches.[67] Rejecting that "[m]odern cell phones are . . . just another technological convenience," *Riley* held that these devices contain the essential "privacies of life" that the Founders fought for.[68]

But behind *Riley*'s melody lay a familiar rhythm—a call to defer to legislative action. Justice Alito filed a concurring opinion conceding that, although the balance the Court had struck between law enforcement and privacy would create legal anomalies, he could "not see a workable alternative" given the need for "clear rules regarding searches incident to arrest."[69] Nevertheless, he warned against using "the blunt instrument of the Fourth Amendment" to protect electronic privacy, particularly since courts are "poorly positioned to understand and evaluate" the "very sensitive privacy

---

'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 government interests.' " (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999))).

The "trilogy" of cases the Court analyzed included *Chimel v. California*, 395 U.S. 752, 762–63 (1969) (holding a warrantless search incident to a lawful arrest to be reasonable if performed "to remove any weapons that the [arrestee] might seek to use in order to resist arrest or effect his escape" or "to prevent . . . concealment or destruction" of evidence, whether "on the arrestee's person" or "the area 'within his immediate control' "), *United States v. Robinson*, 414 U.S. 218, 235–36 (1973) (permitting a search incident to lawful arrest as reasonable despite a low probability in a particular case "that weapons or evidence would in fact be found upon the person of the suspect"), and *Arizona v. Gant*, 556 U.S. 332, 338, 343 (2009) (recognizing the officer safety and evidence preservation concerns and authorizing a warrantless search of a vehicle incident to an arrest "only when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search"). *Riley*, 573 U.S. at 382–85.

64. *Riley*, 573 U.S. at 387–88. The Court also addressed arguments concerning remote data wiping and encryption, finding them inadequate to permit police to search a phone's contents upon arrest absent exigent circumstances. *Id.* at 388–89.

65. *Id.* at 392 (quoting Maryland v. King, 569 U.S. 435, 463 (2013)).

66. *Id.* at 392, 396.

67. *Id.* at 393. *Riley* went further than *Cotterman* in some respects, enumerating additional factors raising privacy concerns, including that "a cell phone collects in one place many distinct types of information . . . that reveal much more in combination than any isolated record" and that "the data on a phone can date back to the purchase of the phone, or even earlier." *Id.* at 394.

68. *Id.* at 403.

69. *Id.* at 407 (Alito, J., concurring in part and concurring in the judgment).

interests" modern technology implicates.[70] For Justice Alito, Congress had demonstrated itself able to respond to those concerns[71] and react to technological changes and their privacy implications.[72] Justice Alito's call would be taken up in the lower courts as they began to decide border search cases in the wake of *Riley*.

C. *The Circuits Split over* Riley

Relying on *Riley*, the Fourth Circuit threw in with the Ninth Circuit and held that a forensic search at the border requires at least reasonable, individualized suspicion.[73] In *United States v. Kolsuz*, customs agents detained the defendant, bound for Turkey from the United States, after finding gun parts in his luggage.[74] The agents seized his smartphone and sent it off-site for forensic analysis, which uncovered a massive amount of personal data.[75] The Fourth Circuit first addressed the threshold issue of whether the search was incident to the defendant's arrest (and therefore squarely within *Riley*'s warrant requirement) or a border search.[76] The court then reviewed case law prior to *Riley*, including *Flores-Montano*'s admonition that "even at the border, individualized suspicion is necessary to justify certain 'highly intrusive searches.' "[77] The court also considered the Ninth Circuit's holding that the scale and sensitivity of information subject to exposure during a forensic search,[78] not to mention the ubiquity of electronic devices,[79] required reasonable suspicion. And if the panel believed that a plausible argument for a suspicion requirement existed even before *Riley* came down, the Supreme Court's reasoning in that case only confirmed it.[80] Although the Fourth Circuit ultimately punted on the question of whether the government needed

---

70. *Id.* at 408.

71. *Id.* To use his example, it did so by passing Title III, sec. 802, of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90–351, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510–20 (2012 & Supp. 2018)), after the Court announced the reasonable expectation of privacy test in *Katz v. United States*, 389 U.S. 347 (1967).

72. *Riley*, 573 U.S. at 408 (Alito, J., concurring in part and concurring in the judgment).

73. United States v. Kolsuz, 890 F.3d 133, 144 (4th Cir. 2018).

74. *Id.* at 136.

75. *Id.* at 139 ("[T]he data extraction process lasted for a full month[] and yielded an 896-page report that included Kolsuz's personal contact lists, emails, messenger conversations, photographs, videos, calendar, web browsing history, and call logs, along with a history of Kolsuz's physical location down to precise GPS coordinates.").

76. *Id.* at 136–37. The court held it was a border search. *Id.* at 144.

77. *Id.* at 144 (quoting United States v. Flores-Montano, 541 U.S. 149, 152 (2004)).

78. *Id.* at 144–45. Because Kolsuz's phone contained his GPS location data, the court also drew on Justice Sotomayor's mosaic concern from *Jones*. *Id.* at 145.

79. *Id.* at 145 ("[I]t is neither 'realistic nor reasonable to expect the average traveler to leave his digital devices at home when traveling.' " (quoting United States v. Saboonchi, 990 F. Supp. 2d 536, 556 (D. Md. 2014))).

80. *Id.* at 144–45.

merely reasonable suspicion or as much as probable cause,[81] forensic searches at the border became subject to at least the reasonable suspicion standard in another circuit.

Still, doubts about the judiciary's role in regulating digital privacy—like those informing Justice Alito's concurrence in *Riley*—motivated one member of the *Kolsuz* panel. Concurring only in the judgment, Judge Wilkinson expressed grave concern that the court had unilaterally struck a constitutional balance on border searches, "where there is a longstanding historical practice . . . of deferring to the legislative and executive branches."[82] Judge Wilkinson argued that, especially given the perils of terrorism, courts put American lives in jeopardy by giving insufficient weight to security interests.[83] It would be more appropriate, Judge Wilkinson argued, to allow Congress and the Executive to make such determinations, because they are entrusted with the same responsibility to uphold the Constitution and are better positioned than the judiciary to evaluate the perils of technology at the border.[84]

The Eleventh Circuit decided *United States v. Touset*[85] just five days after *Kolsuz*. The *Touset* court held that the government needs no suspicion to conduct a forensic search of an electronic device at the border.[86] Putting the circuit at odds with the Fourth and Ninth Circuits, the opinion nonetheless resonated with Justice Alito's and Judge Wilkinson's arguments that the political branches, not the courts, should set the balance between digital privacy and border security.[87]

But the *Touset* opinion did not just focus on the proper role of the courts in national security; it broke sharply with the Fourth and Ninth Circuits' readings of Supreme Court precedent. Relying on the longstanding sovereign power to exclude, the panel interpreted prior case law to mean that all property searches at the border were reasonable without any suspicion.[88] Mr. Touset's attempt to invoke *Riley* failed to persuade the court. Although he had been lawfully arrested, the government's forensic search of his devices was incident to his border crossing, not his arrest (indeed, he was arrested only after the forensic search revealed child pornography).[89] The court saw *Riley* as "expressly limited . . . to the search-incident-to-arrest exception"

81. *Id.* at 147.

82. *Id.* at 153 (Wilkinson, J., concurring in the judgment).

83. *Id.* at 152.

84. *Id.* at 152–53.

85. 890 F.3d 1227 (11th Cir. 2018).

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

87. *Id.* at 1236–37.

88. *Id.* at 1233 ("We see no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property.").

89. *Id.* at 1230.

without applicability to border searches.[90] The court further viewed *Riley* as inapposite because it saw the need for border searches "unencumbered by judicial second-guessing" to be heightened, not lessened, by the presence of electronic devices at the border.[91] Digital contraband such as child pornography "poses the same exact 'risk' of unlawful entry at the border as its physical counterpart," if not a greater risk because of how easily and cheaply it can be smuggled into the country.[92] And if the government's interest in searching electronic devices is greater, surely the level of suspicion needed for those searches cannot be greater.

* * *

Riley strongly suggested that the individual privacy interests in cell phone data are much stronger than those same interests in physical objects on one's person. Yet the circuit courts have disagreed about how those heightened interests interact with the already recognized strong government interests at the border—the Fourth Circuit finding a need for at least reasonable suspicion before permitting a forensic search and the Eleventh Circuit finding no need for suspicion. And in *Riley*, *Kolsuz*, and *Touset*, there remained the refrain that Congress and the Executive are better suited than the courts to strike the balance between privacy and government interests. As discussed in Part III, however, just a month after *Kolsuz* and *Touset*, *Carpenter v. United States*[93] resolved the split.

III. THE CASE FOR PROBABLE CAUSE AND A WARRANT

Carpenter decided that government inspection of a person's cell-site location data is a Fourth Amendment search.[94] Although the police action in *Carpenter* differed in many ways from a border search—few would deny that CBP's inspection of computer files is a Fourth Amendment search—the Court's rationale recognizes strong privacy rights in data affecting the calculus courts must consider for border searches. This Part argues that, based on the reasoning developed in *Jones*, *Riley*, and *Carpenter*, the government must develop probable cause and obtain a warrant before performing a forensic search of an electronic device at the border.

Section III.A responds to Justice Alito's argument in *Riley*, later echoed in the *Kolsuz* dissent and *Touset* majority, that the courts should defer to Congress and the Executive in balancing constitutional rights and the government's interest in national security at the border. The Section contends that the courts should set a baseline level of Fourth Amendment protection

90. *Id.* at 1234 (quoting United States v. Vergara, 884 F.3d 1309, 1312 (11th Cir. 2018)).

91. *Id.* at 1235.

92. *Id.*

93. 138 S. Ct. 2206 (2018).

94. *Id.*

to check potential abusive behavior by the political branches. Section III.B synthesizes Supreme Court case law to define the appropriate factors in weighing the interests of the government and the individual in data searches. Section III.C argues that the requirements of probable cause and a warrant strike the right balance for forensic border searches in light of those factors. Finally, Section III.D applies the rationale of the previous three Sections to other kinds of border searches to sketch arguments for the proper standards of suspicion in those cases.

A. *The Courts Are Right to Decide This Question*

Before arriving at the merits of the argument for probable cause, it is necessary to explain why the judicial branch is the correct forum for this decision. Justice Alito's point is well taken that legislatures are often better situated to "assess and respond to" evolving technology and societal circumstances.[95] Whereas courts must wait for a case to arise involving a new technology to consider the law's application to that technology, legislatures and executive agencies can proactively craft statutes and regulations to address legal implications of a technology before cases even arise.[96] Nor do courts have the same resources to investigate changes in society or technology. They lack the authority and finances to convene expert committees, often rely on litigants to present their own experts,[97] and face external time constraints. By contrast, legislatures and executive agencies frequently convene expert panels and consult their own research staff to make recommendations on proposed statutes and rules, and they can more readily access classified information bearing on national security issues.[98] The political branches regularly seek public comment, while courts are instead isolated decisionmakers, relying on parties and amicus briefs to make decisions. Indeed, Congress and the Executive have proved themselves capable of making such determinations. As Justice Alito pointed out in his *Riley* concurrence, Congress enacted legislation establishing comprehensive procedures to govern the authorization of wiretaps just a year after the Court issued its landmark *Katz v. United States* opinion on the topic.[99] And CBP has already issued

95. Riley v. California, 573 U.S. 373, 408 (2014) (Alito, J., concurring in part and concurring in the judgment).

96. *See, e.g.*, LISA SCHULTZ BRESSMAN ET AL., THE REGULATORY STATE 96–97 (2d ed. 2013).

97. *See, e.g.*, *id.* at 96; John H. Langbein, *The German Advantage in Civil Procedure*, 52 U. CHI. L. REV. 823, 826 (1985).

98. *See, e.g.*, BRESSMAN ET AL., *supra* note 96, at 96–97. *But see* Shirin Sinnar, *Procedural Experimentation and National Security in the Courts*, 106 CALIF. L. REV. 991 (2018) (challenging the idea that courts are ill-equipped to decide national security cases).

99. *See supra* note 71 and accompanying text.

guidelines for border searches of electronic devices; the guidelines require reasonable suspicion before conducting a forensic search.[100]

But even if courts have a more limited capacity to evaluate the impact of technology on privacy, society, and national security, they remain invaluable in striking the constitutional balance at the border. The political branches are far from the "neutral and detached" magistrates who make findings of probable cause to issue warrants.[101] Instead, they operate under a popular mandate to seek out and prevent threats to national security.[102] The courts dampen the passions of the majority by identifying fundamental societal values in the Constitution that must be preserved despite opposing political pressure.[103] Because they are insulated from electoral politics by lifetime tenure, the courts can take a longer view than politicians and stop policies, even popular ones, that would abridge constitutional protections.[104]

If courts declined to review the constitutionality of border searches, there would be no external deterrent to arbitrary, discriminatory, and harassing searches. Nor could those whose rights are violated seek legal redress. Most challenges against illegal searches are brought by criminal defendants whose seized devices contained contraband; those whose devices come up clean have little incentive to sue.[105] And because those charged with crimes after illegal searches often lack political power and popularity, Congress will less likely choose to clamp down on executive overreach.[106] The political ratchet operates in just one direction—in favor of controlling crime and increasing security[107]—and the insulated courts are the only real friction on that ratchet. Therefore, the courts should review actions at the border for reasonableness and impose a sanction if those actions do not meet that basic

100. U.S. CUSTOMS & BORDER PROT., CBP DIRECTIVE NO. 3340-049A, BORDER SEARCH OF ELECTRONIC DEVICES 5 (2018) [hereinafter CBP DIRECTIVE] ("In instances in which there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern . . . an Officer may perform an advanced search of an electronic device.").

101. Shadwick v. City of Tampa, 407 U.S. 345, 350 (1972).

102. *Cf.* Johnson v. United States, 333 U.S. 10, 14 (1948) (referring to law enforcement's "often competitive enterprise of ferreting out crime"); United States v. Lefkowitz, 285 U.S. 452, 464 (1932) ("Security against unlawful searches is more likely to be attained by resort to search warrants than by reliance upon the caution and sagacity of petty officers while acting under the excitement that attends the capture of persons accused of crime.").

103. *See, e.g.*, 1 BRUCE ACKERMAN, WE THE PEOPLE 60 (1991) ("[The Court's] job is to preserve the higher law solutions reached by the People against their erosion during periods of normal politics."); Philip Bobbitt, *Constitutional Fate*, 58 TEX. L. REV. 695, 733–34 (1980) (arguing that courts already decide cases based on "ethical arguments" and should be more transparent about this fact).

104. BRESSMAN ET AL., *supra* note 96, at 97.

105. *See* Sherry F. Colb, *Innocence, Privacy, and Targeting in Fourth Amendment Jurisprudence*, 96 COLUM. L. REV. 1456, 1481 (1996).

106. *See, e.g.*, William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505, 529–30 (2001).

107. *See generally id.*

constitutional standard. Just as courts serve as an essential check on police action inside the country's borders, they must do the same at the border.

B. Jones, Riley, *and* Carpenter *Recognize Strong Fourth Amendment Privacy Interests in Data*

This Note argues that probable cause and a warrant are needed for forensic searches at the border. As no court has ever imposed this standard for border searches, it is important to show why the Supreme Court's recent line of decisions not only permits this doctrinal change but also *requires* it. This Section analyzes the consistent line toward strong data privacy interests running through recent Court decisions, starting with Justice Sotomayor's concurrence in *Jones*, continuing through *Riley*, and culminating in *Carpenter*. This analysis reveals that the Court's primary concern is large-scale government accumulation of personal data that could lead to a later loss of other constitutional rights.

Justice Sotomayor's concurrence in *Jones* espoused a mosaic theory of the Fourth Amendment. The theory posits that, where the government can collect enough individual observations on a person to form a picture of that person's private activities and beliefs—a picture invisible to one not privy to the same wealth of information—it can use that information to chill, passively or actively, "associational and expressive freedoms."[108] Justice Sotomayor suggested that this fear of totalitarian surveillance and suppression might warrant judicial reconsideration of longstanding principles such as the public-thoroughfares doctrine and the third-party doctrine.[109] Importantly, she also recognized the danger of the government's indefinite retention of private data.[110]

Riley embraced and extended Justice Sotomayor's mosaic theory. Chief Justice Roberts identified the storage capacity of a cell phone as a key factor differentiating it from physical containers with respect to searches. That storage capacity lets cell phones "collect[] in one place many distinct types of information . . . that reveal much more in combination than any isolated record."[111] In line with Justice Sotomayor's *Jones* concurrence, Chief Justice Roberts found it troublesome that a cell phone search can reconstruct "[t]he

---

108. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

109. *See id.* ("I do not regard as dispositive the fact that the government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques."); *see also id.* at 417 ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

For the public-thoroughfares doctrine, see generally *California v. Ciraolo*, 476 U.S. 207, 213 (1986) ("The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares."). For the third-party doctrine, see generally *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979).

110. *See supra* note 51 and accompanying text.

111. Riley v. California, 573 U.S. 373, 394 (2014).

sum of an individual's private life . . . through a thousand photographs labeled with dates, locations, and descriptions."[112] Ultimately, the *Riley* Court carved out an exception to the longstanding doctrine permitting searches incident to arrest: the mere fact that a device was on an arrestee's person did not excuse the arresting officer from developing sufficient probable cause and "get[ting] a warrant" to search that device.[113] *Riley* found a historical doctrine based on obsolete considerations unsuited to the modern age.

If there were any remaining doubts about the Court's direction on digital privacy rights, *Carpenter* resolved them. Again writing for the Court, Chief Justice Roberts echoed Justice Sotomayor's *Jones* concurrence, finding that a central aim of the Framers in crafting the Fourth Amendment was "to place obstacles in the way of a too permeating police surveillance."[114] He recalled *Riley*'s holding that the "immense storage capacity" of a cell phone required a warrant despite the search-incident-to-arrest doctrine: "neither of its rationales has much force" in the new context.[115] He also cited prior decisions leaving open whether longstanding doctrine should be reevaluated in light of new technologies.[116]

Carpenter declined to apply the categorical third-party rule to cell-site location information. Chief Justice Roberts distinguished "detailed, encyclopedic, and effortlessly compiled" cell-site location information from bank statements "exposed to [bank] employees in the ordinary course of business" and the "limited capabilities" of a pen register to record outgoing phone numbers.[117] He criticized the government's position as "fail[ing] to contend with the seismic shifts in digital technology that made possible the tracking

112. *Id.*

113. *Id.* at 403.

114. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)). Compare with *United States v. Jones*, 565 U.S. 400, 416–17 (2012) (Sotomayor, J., concurring) ("I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercises of police power and prevent 'a too permeating police surveillance.' " (quoting United States v. Di Re, 332 U.S. 581, 595 (1948))).

115. *Carpenter*, 138 S. Ct. at 2214 (quoting *Riley*, 573 U.S. at 386, 393).

116. *E.g.*, *id.* at 2215 ("[T]he Court reserved the question whether 'different constitutional principles may be applicable' if 'twenty-four hour surveillance of any citizen of this country [were] possible.' " (second alteration in original) (quoting United States v. Knotts, 460 U.S. 276, 283–84 (1983))); *id.* (" '[L]onger term GPS monitoring in investigations of most offenses impinges on expectations of privacy'—regardless whether those movements were disclosed to the public at large." (quoting United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring in the judgment))).

117. *Id.* at 2216 (alteration in original) (quoting United States v. Miller, 425 U.S. 435, 442 (1976), and Smith v. Maryland, 442 U.S. 735, 742 (1979)). But, as Justice Kennedy noted, "The troves of intimate information the Government can and does obtain using financial records and telephone records dwarfs what can be gathered from cell-site records." *Id.* at 2232 (Kennedy, J., dissenting). Even so, the point remains that the Court's ultimate concern was with the amount and intimacy of data collected.

of" someone's location "not for a short period but for years and years."[118] He painted a picture of an Orwellian panopticon, "ever alert" with "nearly infallible" memory, capable of tracking "any activity on [a] phone," a device he once again described as "indispensable to participation in modern society."[119] Because the records at issue created a "detailed chronicle of a person's physical presence compiled every day, every moment, over several years,"[120] they were sufficiently different from the records in prior third-party doctrine cases to justify a break from the hard rule of the past.

From *Jones* through *Carpenter*, the key question driving the Court in electronic search cases has been whether some instance of surveillance (including retention of its results) is quick enough, cheap enough, and scalable enough to create the potential for a dystopian nightmare leading to the loss of basic political and expressive freedoms. If so, then there must be sufficient procedural barriers to ensure that, in light of the government's interests, that surveillance is reasonable.

C. *Requiring Probable Cause and a Warrant Correctly Balances Interests in Light of* Jones*,* Riley*, and* Carpenter

Using the principles extracted from the decisions above, this Section analyzes the balance between government border security interests and individual privacy interests, concluding that probable cause is necessary for the government to conduct a forensic search. This Section further considers the potential for government agents to abuse the power to search electronic devices without probable cause. It argues that judicial enforcement is needed to deter arbitrary, discriminatory, and harassing forensic searches.

A short diversion at this point is warranted. Why is interest balancing the correct method of analysis here—why not look to historical understandings of reasonableness as done in *Boyd*, *Ramsey*, or *Touset*? In short, the present has obsoleted notions of what was once reasonable. When *Boyd* was decided in 1886, the property crossing the border was not much different than a century before at the Founding, so historical understandings of reasonableness mapped well onto then-current practices. But dramatic technological progress since 1886—and the Founding—now forecloses using comparable circumstances in Fourth Amendment decisionmaking. Accordingly, in cases like these, where historical understandings do not neatly track modern realities, the Court regularly engages in interest balancing to resolve constitutional questions.[121]

That said, it remains to conduct the interest analysis for reasonableness. Requiring probable cause before conducting a forensic search imposes only a minor burden on the government. A border agent need only identify factors

118. *Id.* at 2219.

119. *Id.* at 2220–21 (citing Riley v. California, 573 U.S. 373, 385 (2014)).

120. *Id.*

121. *See supra* note 63 and accompanying text.

that, in the aggregate, lead to a " 'substantial basis for . . . conclud[ing]' that a [forensic] search would uncover evidence of wrongdoing."[122] The factors present in the cases discussed above—a past conviction for possessing child pornography or an open investigation on export violations, combined with recent travel through countries known to be hotspots for sex trafficking or terrorism—support reasonable suspicion for a nonforensic search.[123] If that search turned up suspicious files, probable cause for a deeper forensic search would likely develop. And the burden on government agents to obtain a warrant would be minimal: after developing probable cause, a border official may seize the suspicious device pending a warrant.[124]

Further, requiring border agents to develop probable cause before forensically searching a traveler's device would likely not affect national security interests appreciably. Because a forensic search takes so much time to complete,[125] it is unlikely to turn up evidence of drugs, weapons, or other tangible contraband items before a criminal has already cleared the border and brought them into the country. And because no suspicion is needed to conduct physical searches of luggage at the border or to use drug- or bomb-sniffing dogs at airports,[126] a probable cause requirement for digital data will not reduce border agents' ability to seize physical contraband. As for electronic contraband, imposing a constitutional barrier of probable cause before seizing a device for forensic inspection would likely let in little more—if any—illegal data. Indeed, any electronic data stopped at the border would likely find another path into the country through the internet,[127] so border searches are not an effective shield against electronic contraband.[128] In fact,

---

122. Illinois v. Gates, 462 U.S. 213, 236 (1983) (quoting Jones v. United States, 362 U.S. 257, 271 (1960)).

123. See *infra* Section III.D for a discussion of why nonforensic searches should require reasonable suspicion.

124. *Cf.* Kentucky v. King, 563 U.S. 452, 462–63 (2011) (permitting police to enter a home and seize evidence to prevent its destruction, provided the police did not violate the Constitution leading up to the entry and seizure).

125. *But see supra* note 39. If technology developed for quickly detecting evidence of physical contraband through a mobile phone or laptop search, the social burden of imposing a probable cause requirement would increase. However, depending on the nature of the technology and whether it stored information about files it searched, the intrusion on individual privacy might increase as well.

126. United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985); United States v. Place, 462 U.S. 696, 698 (1983).

127. Ari B. Fontecchio, Note, *Suspicionless Laptop Searches Under the Border Search Doctrine: The Fourth Amendment Exception that Swallows Your Laptop*, 31 CARDOZO L. REV. 231, 250–51 (2009) ("Data, on the other hand, may readily enter the U.S. within seconds from anywhere in the world without stopping at a physical border. Data is intangible; it can be copied easily and moved quickly from one computer to another.").

128. And to the extent we are concerned less with stopping the data than stopping criminals from entering the country, this sounds a lot more like a "general interest in law enforcement" that ordinarily requires probable cause. *See* Ferguson v. City of Charleston, 532 U.S. 67, 79 (2001).

the probable cause requirement may actually reduce the overall burden on the government. A thorough forensic search may take hours, days, or months; requiring probable cause would redirect those resources to searches more likely to be fruitful.[129]

By contrast, the individual interests at stake are enormous. Forensic searches copy the entire contents of a person's device, including private photos, videos, text messages, notes, call records, locational data, search queries, and browser histories.[130] All this data would almost certainly reveal a "wealth of detail about [a person's] familial, political, professional, religious, and sexual associations."[131] And from the graveyard of unallocated disk space, the government can even resurrect data that a user had intended to delete.[132] Especially troubling is that data that may have been deleted precisely to prevent its exposure to prying government eyes at a border checkpoint. Forensic access to this deleted information comes dangerously close to giving government agents the power to copy a person's innermost thoughts and retain them indefinitely—an Orwellian panopticon if there ever were one.

Requiring probable cause and a warrant for a forensic search is also necessary to prevent arbitrary, discriminatory, and harassing searches. Government agents, even at their best, are human and make mistakes. At their worst, they succumb to bias and prejudice, detaining and searching people fitting a particular ethnic or religious profile. Border agents have detained U.S. citizens merely for speaking a foreign language[133] and have disproportionately strip-searched people based on race and gender.[134] Allowing agents unfettered discretion to decide which border travelers should have their devices screened in a forensic search will lead to unjust profiling. Instead, requiring affidavits for warrants based on probable cause will force border agents to articulate their reasons for suspecting a person, and requiring a

129. Fontecchio, *supra* note 127, at 248–49.

130. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 540 (2005) ("To ensure the evidentiary integrity of the original evidence, the computer forensics process always begins with the creation of a perfect 'bitstream' copy or 'image' of the original storage device saved as a 'read only' file.").

131. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

132. Kerr, *supra* note 130, at 542–43.

133. *E.g.*, Farag v. United States, 587 F. Supp. 2d 436, 443–46 (E.D.N.Y. 2008) (U.S. citizen of Egyptian origin detained after speaking Arabic with Egyptian friend on domestic flight); Grace Panetta, *The US Border Patrol Could Be Facing a Lawsuit After 2 US Citizens Say They Were Detained for Speaking Spanish*, BUS. INSIDER (May 24, 2018, 5:35 PM), https://www.businessinsider.com/border-patrol-racial-profiling-lawsuit-2018-5 [https://perma.cc/R7FF-Q66W].

134. *E.g.*, U.S. GEN. ACCOUNTING OFFICE, GAO/GGD-00-38, U.S. CUSTOMS SERVICE: BETTER TARGETING OF AIRLINE PASSENGERS FOR PERSONAL SEARCHES COULD PRODUCE BETTER RESULTS 12 & tbl.3 (2000) (showing that black women were more likely to be strip-searched than other racial and gender groups).

magistrate's approval will forestall invading someone's privacy on the basis of a single agent's prejudice.[135]

A probable cause requirement would also mitigate the problem of data retention. Currently, government agencies that collect such intimate data also determine how long they can retain it. Although current CBP policy is to destroy data obtained during a forensic search if no probable cause develops from the search,[136] there is only the agency's word that it will do so. CBP could change its policy in response to heightened security concerns. Or perhaps the CBP guidelines will be—or already are—superseded by a secret executive order, purporting to rely on inherent Article II authority, to retain any forensically obtained data indefinitely.[137] Even if the data is kept ostensibly for national security reasons, it remains ready to be used by a malevolent government actor. Storing data is cheap,[138] and presidents of all partisan stripes have pushed the boundaries of constitutionality in the name of national security.[139] The best way to prevent the government from preserving innocent travelers' private data is to prohibit gathering it at the outset without probable cause and a warrant from a neutral magistrate.

Just as in *Riley* and *Carpenter*, a longstanding doctrine of the past gives the government great discretion in deciding to conduct a search. But precisely because it is longstanding, the border search doctrine is the product of a time without the possibility of pervasive police surveillance. The Court has held that historical practices cannot reasonably grant the government carte blanche to copy and retain the immense amount of information stored in a person's digital devices. Far more so than GPS data and cell-site location information, a cell phone or laptop's contents tell a "detailed chronicle" of someone's life over the span of months or years.[140] The Executive, armed with forensic software, "a tool so amenable to misuse," requires "oversight from a coordinate branch . . . to curb arbitrary exercises of police power."[141] And for the same reasons articulated in *Riley*, a warrant is necessary for the

135. *See* Oren Bar-Gill & Barry Friedman, *Taking Warrants Seriously*, 106 NW. U. L. REV. 1609, 1614 (2012).

136. CBP DIRECTIVE, *supra* note 100, at 7, 10.

137. *Cf.* Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html [https://perma.cc/KMM8-H5N2] (describing the PRISM program, revealed by the Snowden leaks and which warrantlessly collected "the content of innocent Americans who were swept up in a search for someone else").

138. Google currently charges 2.6 cents per gigabyte of data per month for its cloud computing storage. *Cloud Storage Pricing*, GOOGLE CLOUD, https://cloud.google.com/storage/pricing [https://perma.cc/ZT2L-VT79].

139. *See* Paul Szoldra, *This Is Everything Edward Snowden Revealed in One Year of Unprecedented Top-Secret Leaks*, BUS. INSIDER (Sept. 16, 2016, 8:00 AM), https://www.businessinsider.com/snowden-leaks-timeline-2016-9 [https://perma.cc/DP9A-2X67].

140. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

141. United States v. Jones, 565 U.S. 400, 416–17 (2012) (Sotomayor, J., concurring).

Executive to responsibly deploy such a tool: warrants are "an important working part of our machinery of government," needed to combat the excesses represented by the writs of assistance the Founders rebelled against.[142] Thus, the "quantitative" and "qualitative" differences in the nature of electronic data[143] defy the assumptions justifying the border search doctrine. Not then, but now, the probable cause standard is needed to protect "the privacies of life."[144] The rationale driving *Jones*, *Riley*, and *Carpenter* requires this outcome.

D. *Why Not Require Probable Cause for Other Intrusive Border Searches?*

If probable cause is required for forensic border searches, though, why not a higher standard for other border searches? Indeed, the logic of this Part compels the conclusion that some other border searches must have higher standards of suspicion than courts currently require. This last Section examines the implications of the *Jones–Riley–Carpenter* line on border searches of property, intrusive searches of the person, and nonforensic searches of electronic devices.

For searches of tangible, nonelectronic property, this line of cases gives little guidance. It is unlikely that a massive amount of intimate data like that on an electronic device would ever pass through the border in physical documents.[145] The privacy concerns implicated by forensic searches simply do not apply to searches of luggage, of a vehicle, or even generally of one's person. As for particularly intrusive searches of the person, the reasonable suspicion standard may still provide a proper balance.[146] If a person is reasonareasonably suspected of carrying drugs or explosives, there is greater urgency for the government to search that person—both because of the tangible harms the contraband can cause inside the country and because of its inability to cross the border except at physical ports, unlike data.[147]

But for nonforensic searches, the balance of interests requires a change to the status quo of suspicionless searches. Although *Jones* and *Carpenter* primarily concern systemic, pervasive police surveillance that can piece to-

142. Riley v. California, 573 U.S. 373, 401–03 (2014) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971)).

143. *Id.* at 393.

144. *Id.* at 403 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

145. It seems improbable such a case would ever reach the courts, either. Even if a traveler brought into the country a literal warehouse's worth of hard-copy documents and photographs, unless she were a high-profile international criminal, the government would hardly want to expend the resources to copy each of those physical documents individually.

146. I hesitate here because of the real, lasting psychological harm a forced strip-search or cavity search can cause. Perhaps a warrant based on probable cause would be better for those searches; that question is beyond the scope of this Note. But reasonable suspicion does seem like a fair standard for machine-based searches, like abdominal x-rays or microwave scans, from which probable cause could develop.

147. Fontecchio, *supra* note 127, at 249–52.

gether a person's secrets, *Riley* still teaches that "unbridled discretion to rummage at will among" even a few messages or pictures on a cell phone is highly intrusive, especially if the searched data "date[s] back to the purchase of the phone, or even earlier."[148] Indeed, the police searches in *Riley* had a similar scope to a nonforensic border search, and the Court found the *Riley* searches to require a warrant.[149] Thus, in balancing the government and individual interests at issue in nonforensic searches, courts must consider the deeply intrusive nature of even a cursory phone inspection.

The government interest at stake in a nonforensic search is primarily, as with a forensic search, to exclude physical contraband from entry. But a nonforensic search takes a fraction of the time to conduct, and a customs agent could use the fruits of that search to immediately prevent contraband's entry. Accordingly, the government's interest in performing nonforensic searches is higher than for forensic searches. On the other side of the scale, as the Court indicated in *Riley*, the privacy intrusion inherent in a nonforensic search is serious—in the league of the general warrant.[150] Even so, the intrusion is not nearly as severe as with a forensic search: files are manually inspected but not copied or retained. There is not the same danger of a pervasive police surveillance.

Given the increased government burden from lost opportunities to conduct nonforensic border searches and the reduced intrusion on individual privacy, probable cause is too high a standard. But to require no suspicion at all would ignore *Riley*'s grave concerns with the government's ability to search a person's electronic data at will. Therefore, the appropriate balance is reasonable, articulable suspicion that a person's device will contain evidence of contraband.[151]

CONCLUSION

The border search doctrine establishes a sovereign right to exclude unwanted persons and things, in effect making almost any search at the border "reasonable." But the doctrine creates a categorical rule unsuited for the modern era. The Supreme Court has recognized in three recent cases that government accumulation of large amounts of personal data, even through otherwise lawful searches, strips individuals of their rightful privacy and

148. *Riley*, 573 U.S. at 399, 394–99 (quoting Arizona v. Gant, 556 U.S. 332, 345 (2009)).

149. *Id.* at 403.

150. See, for example, *id.* and *Stanford v. Texas*, 379 U.S. 476, 481–82 (1965), each citing a 1761 speech by James Otis that denounced the writs of assistance and quoting John Adams's response. Adams wrote that "[e]very man of a crowded audience appeared to me to go away, as I did, ready to take arms against writs of assistance" and that the speech was "the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born." 10 WORKS OF JOHN ADAMS 247–48 (C. Adams ed., 1856).

151. *See* Terry v. Ohio, 392 U.S. 1, 21 (1968) ("[I]n justifying the particular intrusion the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion.").

gives the government a tool to facilitate further constitutional violations. Applying this rationale to forensic searches at the border makes clear that, just as other longstanding exceptions to the probable cause and warrant requirements have yielded in the face of electronic data privacy, the border search doctrine too must yield. Setting the proper balance of government and individual interests in electronic data requires that the government develop probable cause and seek a warrant for such an intrusive search into a person's data.