Washington Law Review

Volume 90 | Number 4

12-1-2015

Digital Border Searches after *Riley v. California*

Thomas Mann Miller

DIGITAL BORDER SEARCHES AFTER *RILEY v. CALIFORNIA*

Thomas Mann Miller*

Abstract: The federal government claims that the Fourth Amendment permits it to search digital information on cell phones, laptops, and other electronic devices at the international border without suspicion of criminal activity, much less a warrant. Until recently, federal courts have generally permitted these digital border searches, treating them no differently from searches of luggage. Courts that have limited digital border searches have required only that the government establish reasonable suspicion for the most exhaustive kind of digital search. The Supreme Court has not yet weighed in, but last year it held in *Riley v. California* that the search incident to arrest exception to the warrant requirement does not apply to cell phones. This Comment analyzes how *Riley* affects the border search doctrine and concludes that it should change the debate in significant ways. First, *Riley* establishes that digital searches are categorically different from physical searches. This undermines the first wave of border search decisions and suggests that courts will have to analyze digital searches differently. Second, the Court recognized that digital searches could be even more intrusive than the search of one's home. This finding weighs in favor of requiring at least reasonable suspicion, if not probable cause, for digital border searches. Third, the Court provides a test for determining when to deviate from the warrant requirement in light of new technology. The Court's analysis on this question supports reconsidering whether the border search exception—traditionally applied to searches of persons and physical property—should apply to searches of digital information.

INTRODUCTION

Despite a variety of important individual interests in digital information, U.S. border agents seize and search cell phones, laptop computers, and other electronic devices of people entering and exiting the country without any suspicion of criminal activity.[1] This is pursuant

* The author interned for the American Civil Liberties Union of Northern California in 2014 and the Brennan Center for Justice at New York University School of Law in 2015. Both organizations have taken positions on digital border searches, but the author did not work for either organization on this issue. The views expressed in this Comment are the author's alone.

1. U.S. Customs and Border Protection "has often ignored opposing assertions of attorney-client privilege and Fourth Amendment rights, while pursuing the exercise of its almost unlimited authority to search for illegal materials." Robert T. Givens, *The Danger of U.S. Customs Searches for Returning Lawyers*, GPSOLO, May/June 2013, at 39, 40, *available at* http://www.americanbar.org/publications/gp_solo/2013/may_june/the_danger_us_customs_searches_returning_lawyers.html. "The best policy [for lawyers] is to have nothing on your person or in your baggage that you cannot have the government know about." *Id.* at 41. Border officials recently stopped the Mayor of Stockton, California at San Francisco International Airport and confiscated a

to official policy: U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE) have each passed directives authorizing agents to conduct these digital border searches.[2] The government contends that this intrusive power is justified by a broad interest in enforcing the law at the border,[3] and argues in court that the practice is consistent with the Fourth Amendment's prohibition on unreasonable searches and seizures.[4]

The U.S. Supreme Court has not yet decided what level of process the Fourth Amendment requires for digital border searches, although it has set out general principles governing border searches.[5] The Court has

---

personal cell phone, personal laptop, and city-owned laptop. The mayor was traveling to China on a business tour with other California mayors. Officials allowed him to leave custody only after he provided passwords to the devices. Officials returned the devices about a month later, after the mayor went to federal court. Roger Phillips, *Mayor to Get His Electronics Back*, THE RECORD (Oct. 21, 2015), http://www.recordnet.com/article/20151021/NEWS/151029932. For additional examles of the interests at stake in digital border searches, see Ellen Nakashima, *Clarity Sought on Electronics Searches: U.S. Agents Seize Travelers' Devices*, WASH. POST, Feb. 7, 2008, at A1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/02/06/AR2008020604763_pf.html (recounting story of a technology engineer who was asked by a federal agent to enter his password into his laptop computer and watched as the officer "copied the Web sites he had visited"); Sarah Abdurrahman, *My Detainment Story*, ON THE MEDIA (Sept. 30, 2013), http://www.onthemedia.org/story/my-detainment-story-or-how-i-learned-stop-feeling-safe-my-own-country-and-hate-border-patrol/transcript/ (describing her experience as a Muslim-American journalist during a border search of cell phones); Geoffrey King, *For Journalists Coming into US, Policies Border on the Absurd*, COMM. TO PROTECT JOURNALISTS (Oct. 28, 2014), https://cpj.org/blog/2014/10/for-journalists-coming-into-us-policies-that-borde.php (discussing how journalists have had to change how they work because of invasive digital border searches).

2. *See* U.S. CUSTOMS & BORDER PROT., BORDER SEARCH OF ELECTRONIC DEVICES CONTAINING INFORMATION (2009) [hereinafter CBP DIRECTIVE], *available at* http://www.cbp.gov/sites/default/files/documents/elec_mbsa_3.pdf; U.S. IMMIGRATION & CUSTOMS ENFORCEMENT, ICE DIRECTIVE NO. 7-6.1, BORDER SEARCHES OF ELECTRONIC DEVICES (2009) [hereinafter ICE DIRECTIVE], *available at* http://www.dhs.gov/sites/default/files/publications/7-6.1%20directive.pdf. Although the CBP Directive states that it was subject to review in 2012, it remains listed as current policy. *See CBP Policy Regarding Border Search of Electronic Devices Containing Information*, U.S. CUSTOMS & BORDER PROTECTION, http://www.cbp.gov/document/directives/cbp-policy-regarding-border-search-electronic-devices-containing-information (last visited Sept. 30, 2015).

3. *E.g.*, CBP DIRECTIVE, *supra* note 2, § 1, at 1. "Searches of electronic devices help detect evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography. They can also reveal information about financial and commercial crimes, such as those relating to copyright, trademark and export control violations." *Id.*; *see also id.* § 4, at 2 (citing federal statutes relating to immigration, customs, monetary instruments, and exports).

4. *See, e.g.*, United States v. Cotterman, 709 F.3d 952, 959 (9th Cir. 2013) (the government "sought a broad ruling that no suspicion of any kind was required" for digital border searches); United States v. Kim, No. 13-cr-00100-ABJ, 2015 BL 134375, at *1 (D.D.C. May 8, 2015), *available at* https://cdn.arstechnica.net/wp-content/uploads/2015/05/kimruling.pdf (the government argued that the laptop search was routine and did not require reasonable suspicion).

5. *See infra* Part I.B–C.

held that border officials may conduct "routine" searches of persons and personal property at the border without suspicion of criminal activity or a warrant.[6] The Court has indicated that "nonroutine" searches may require a heightened standard of process.[7] For example, a search that is particularly destructive to personal property or highly intrusive to personal dignity may be nonroutine and require some level of suspicion.[8]

The lower federal courts have faced the difficult task of sorting out how to apply the Supreme Court's border search decisions—which involved searches of physical property and the temporary seizure of persons—to searches of digital information accessible through computers and cell phones. There are two main developments in the case law.[9] At first, most federal courts rejected challenges to digital border searches under the Fourth Amendment and, for the most part, concluded that border agents did not need any level of suspicion.[10]

More recent cases suggest the emergence of a second trend. In 2013, the Ninth Circuit held in *United States v. Cotterman*[11] that the Fourth Amendment requires border agents to show reasonable suspicion of criminal activity before conducting a "forensic" digital search of a computer that could reveal deleted files.[12] In doing so, the court narrowed its 2008 decision in *United States v. Arnold*,[13] in which it had held that no suspicion was required for any digital border search.[14]

---

6. *See infra* Part I.B–C.

7. *See infra* Part I.B–C.

8. *See* United States v. Flores-Montano, 541 U.S. 149, 155–56 (2004) ("While it may be true that some searches of property are so destructive as to require [some level of suspicion], this was not one of them."); *id.* at 152 (identifying "dignity and privacy interests of the person being searched" as "reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person"); *cf.* United States v. Ramsey, 431 U.S. 606, 618 n.13 (1977) ("We do not decide whether, and under what circumstances, a border search might be deemed 'unreasonable' because of the particularly offensive manner in which it is carried out.").

9. *See infra* Part II.

10. *See, e.g.*, United States v. Stewart, 729 F.3d 517, 525–26 (6th Cir. 2013) (concluding that the nonforensic examination of a laptop computer occurring twenty miles away from the international airport was a continuation of a routine border search and did not require reasonable suspicion); United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008) (holding that the Fourth Amendment does not protect electronic devices, including computers and cell phones, from warrantless and suspicionless searches in border context); United States v. Ickes, 393 F.3d 501, 504 (4th Cir. 2005) (same); United States v. Linarez-Delgado, 259 F. App'x 506, 508 (3d Cir. 2007) (stating that there is no reasonable suspicion required for a routine border search of "[d]ata storage media and electronic equipment, such as films, computer devices, and videotapes").

11. 709 F.3d 952 (9th Cir. 2013).

12. *Id.* at 956–57.

13. 533 F.3d 1003 (9th Cir. 2008).

14. *Cotterman*, 709 F.3d at 960 n.6.

Nevertheless, the debate in both lines of cases is limited to whether border officials must meet the lowest level of process required under the Fourth Amendment—reasonable suspicion—before conducting digital border searches.[15]

The United States Supreme Court's decision in *Riley v. California*,[16] should spark a change in the doctrine in significant ways. In *Riley*, the Court declined to extend the search incident to arrest exception to cell phones and held that police officers must obtain a warrant before searching a cell phone incident to arrest.[17] The Court recognized that digital searches are categorically distinct from searches of physical objects.[18] The Court definitively rejected analogies between digital information accessible by cell phones and physical property[19]—one of the principal rationales underlying *Arnold* and other decisions holding that no suspicion is required for a digital border search.[20] This part of the Court's analysis should push lower courts to distinguish digital searches from searches of physical belongings.

The Court also established that digital searches can be more intrusive than even the search of one's home.[21] This weighs in favor of requiring at least reasonable suspicion, if not probable cause, for digital border searches. Finally, and perhaps most significantly, *Riley* provides a test for deciding whether to deviate from the Fourth Amendment's baseline warrant requirement in light of new technology.[22] The Court's analysis on this question supports reconsidering whether to apply the border search exception to digital searches.

While the scholarly debate largely reflects the pre-*Riley* debate analysis in the federal courts over reasonable suspicion,[23] this Comment

---

15. *Id.* at 968–70; *Arnold*, 533 F.3d at 1008.

16. __ U.S. __, 134 S. Ct. 2473 (2014).

17. *Id.* at 2485.

18. *See infra* notes 278–82 and accompanying text.

19. *Riley*, 134 S. Ct. at 2488–89.

20. *Arnold*, 533 F.3d at 1009.

21. *Riley*, 134 S. Ct. at 2491.

22. *See infra* Part III.A.

23. *See* Patrick E. Corbett, *The Future of the Fourth Amendment in a Digital Evidence Context: Where Would the Supreme Court Draw the Electronic Line at the International Border?*, 81 MISS. L.J. 1263 (2012); John Palfrey, *The Public and the Private at the United States Border with Cyberspace*, 78 MISS. L.J. 241 (2008); Samuel A. Townsend, Note, *Laptop Searches at the Border and* United States v. Cotterman, 94 B.U. L. REV. 1745 (2014); Michael Creta, Comment, *A Step in the 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. E-SUPPLEMENT 31 (2014); Matthew B. Kugler, Comment, *The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study*, 81 U. CHI. L. REV. 1165 (2014);

examines the implications of *Riley* and its potential to change how courts assess the reasonableness of digital border searches.[24] In short, *Riley* supports a higher level of process for digital border searches than what courts currently require and impliedly settles the debate over reasonable suspicion for forensic searches. Further, *Riley* opens up a doctrinal path for courts to reconsider whether to extend the border search exception to the warrant requirement—traditionally applied to searches of persons and personal property—to searches of digital information. After *Riley*, courts should require, at a minimum, reasonable suspicion for all digital border searches and perhaps even a warrant supported by probable cause.

Indeed, lower courts are already grappling with differing interpretations of *Riley* in digital border search cases.[25] The Fourth Circuit may be the first federal court of appeals to take on the issue in light of these developments following an appeal filed in *United States v. Saboonchi*.[26] In that case, the defendant and amici argue on appeal that,

---

Sid Nadkarni, Comment, *"Let's Have a Look, Shall We?" A Model for Evaluating Suspicionless Border Searches of Portable Electronic Devices*, 61 UCLA L. REV. 148 (2013); Benjamin Rankin, Note, *Restoring Privacy at the Border: Extending the Reasonable Suspicion Standard for Laptop Border Searches*, 43 COLUM. HUM. RTS. L. REV. 301 (2011); Rachel Flipse, Comment, *An Unbalanced Standard: Search and Seizure of Electronic Devices Under the Border Search Doctrine*, 12 U. PA. J. CONST. L. 851 (2010); Scott J. Upright, Note, *Suspicionless Border Seizures of Electronic Files: The Overextension of the Border Search Exception to the Fourth Amendment*, 51 WM. & MARY L. REV. 291 (2009); Sunil Bector, Note, *Your Laptop, Please: The Search and Seizure of Electronic Devices at the United States Border*, 24 BERKELEY TECH. L.J. 695 (2009); Rasha Alzahabi, Note, *Should You Leave Your Laptop at Home When Traveling Abroad?: The Fourth Amendment and Border Searches of Laptop Computers*, 41 IND. L. REV. 161 (2008); Christine A. Coletta, Note, *Laptop Searches at the United States Borders and the Border Search Exception to the Fourth Amendment*, 48 B.C. L. REV. 971 (2007); Kelly A. Gilmore, Note, *Preserving the Border Search Doctrine in a Digital World: Reproducing Electronic Evidence at the Border*, 72 BROOK. L. REV. 759, 761–64 (2007); *see also* Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193 (2005) (discussing computer searches under the Fourth Amendment more generally).

24. Gretchen C.F. Shappert noted that the government conceded in *Riley* that digital searches incident to arrest "may not be stretched" to include files accessible through a cell phone but stored remotely. Gretchen C.F. Shappert, *The Border Search Doctrine: Warrantless Searches of Electronic Devices After* Riley v. California, 62 U.S. ATT'YS' BULL., Nov. 2014, at 1, 13. She concluded that the same principle would apply to digital border searches, though she did not elaborate as to why: "If a search incident to arrest 'may not be stretched' to cover cloud data, then a routine border search 'may not be stretched' either." *Id.*

25. *See, e.g.*, United States v. Kim, No. 13-cr-00100-ABJ, 2015 BL 134375, at *2 (D.D.C. May 8, 2015), *available at* https://cdn.arstechnica.net/wp-content/uploads/2015/05/kimruling.pdf (holding a digital border search was unreasonable under the *Riley* balancing test analysis); United States v. Saboonchi, 48 F. Supp. 3d 815, 816 (D. Md. 2014) (denying motion for reconsideration in light of *Riley* and affirming holding that reasonable suspicion is required for a forensic search of digital devices seized at the border).

26. 990 F. Supp. 2d 536 (2014); Notice of Appeal, United States v. Saboonchi, No. PWG-13-100,

under *Riley*, the Fourth Amendment requires border agents to obtain a warrant to conduct a digital border search or, at a minimum, establish reasonable suspicion.[27]

This Comment proceeds in three parts. Part I discusses the border search exception generally. Part II discusses digital border searches, focusing on the two major trends in the case law, including a split over whether a search of digital information should be treated differently from a search of physical items. Part III discusses *Riley*, its implications for other digital searches, and how courts have debated *Riley*'s impact on digital border searches thus far. Part III concludes with an analysis of what courts should take away from *Riley* when assessing the constitutionality of digital border searches.

I. BORDER SEARCHES

Every year, millions of people travel into and out of the United States with cell phones, tablets, laptops, digital cameras, and other electronic devices.[28] In 2013, 180 million people took international flights serving the United States.[29] A recent survey found that nearly all (ninety-four percent) of United States adult airline passengers brought at least one portable electronic device with them onto an aircraft while traveling in the past twelve months.[30] In 2014, 236 million people legally entered the United States from Canada and Mexico, traveling in personal vehicles (nearly 189 million), buses (over 5 million), and trains (nearly 295,000),

---

2015 WL 410506 (D. Md. Feb. 24, 2015).

27. Brief of Appellant at 8–9, United States v. Saboonchi, No. 15-4111 (4th Cir. Feb. 25, 2015); Brief of Amicus Curiae American Civil Liberties Union and American Civil Liberties Union of Maryland in Support of Defendant-Appellant at 2–3, *Saboonchi*, No. 15-4111 (Sept. 3, 2015) [hereinafter Brief of Amicus Curiae ACLU]; Brief of Amicus Curiae Electronic Frontier Foundation in Support of Appellant at 4, *Saboonchi*, No. 15-4111 (Sept. 3, 2015) [hereinafter Brief of Amicus Curiae EFF].

28. *See* U.S. FED. AVIATION ADMIN., A REPORT FROM THE PORTABLE ELECTRONIC DEVICES AVIATION RULEMAKING COMMITTEE TO THE FEDERAL AVIATION ADMINISTRATION: RECOMMENDATIONS ON EXPANDING THE USE OF PORTABLE ELECTRONIC DEVICES DURING FLIGHT app. H, at H-8 (2013), *available at* http://www.faa.gov/about/initiatives/ped/media/PED_ARC_FINAL_REPORT.pdf.

29. U.S. DEP'T OF TRANSP., TOTAL PASSENGERS ON U.S AIRLINES AND FOREIGN AIRLINES SERVING THE U.S. INCREASED 1.3% IN 2013 FROM 2012 (2014), *available at* http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/bts13_14.pdf.

30. U.S. FED. AVIATION ADMIN., *supra* note 28. The survey found that twenty-eight percent of travelers used smartphones on flights, twenty-five percent used laptop computers, twenty-three percent used tablets, twenty-three percent used digital audio or MP3 players, and thirteen percent used e-readers. *Id.* app. H, at H-12. Of those traveling with a portable electronic device, ninety-nine percent took at least one device on the plane as a carry-on item. *Id.* app. H, at H-11.

as well as by foot (nearly 42 million).[31]

Almost all adults in the United States own cell phones. In 2012, ninety percent of American adults owned a cell phone.[32] An estimated eighty-five percent of Americans aged eighteen to twenty-four owned a smartphone in 2014.[33] Half of American adults owned either a tablet or an e-reader at the start of 2014.[34] Indeed, smartphones have "outpaced nearly any comparable technology in the leap to *mainstream* use."[35] As one court recently put it: "Smartphones, in particular, have become so deeply embedded in day-to-day activities that travelers cannot reasonably be expected to travel without them."[36]

Americans use personal electronic devices, and smartphones in particular, in personal ways. Smartphones invite users to share information in a variety of ways—from sending and receiving texts, email, and photos to making video calls, managing a calendar, buying things online, and browsing the internet—and people make full use of these functions.[37] An estimated sixty-two percent of Americans used their smartphone to get information about a health condition in the past year and fifty-seven percent have used their smartphone for online banking.[38] Smartphones also gather, retain, and transmit location information. For example, Apple's iPhone logs the frequent locations of

---

31. *Border Crossing/Entry Data: Query Detailed Statistics*, U.S. DEPARTMENT TRANSP., BUREAU TRANSP. STAT., http://transborder.bts.gov/programs/international/transborder/TBDR_BC/TBDR_BCQ.html (last visited Nov. 19, 2015) (select options for "All Border Ports," "2014," "Annual Summary," "Aggregate all Ports," and "All Measures Detail"; then click "Submit" to retrieve data) (based on data from the Department of Homeland Security, U.S. Customs and Border Protection, Office of Field Operations).

32. *Mobile Technology Fact Sheet*, PEW RES. CENTER, http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/ (last visited Mar. 11, 2015) (webpage updated when new data is available; included numbers are current as of January 2014 and are based on 2012 data).

33. *Mobile Millennials: Over 85% of Generation Y Owns Smartphones*, NIELSEN (Sept. 5, 2014), http://www.nielsen.com/us/en/insights/news/2014/mobile-millennials-over-85-percent-of-generation-y-owns-smartphones.html.

34. Kathryn Zickuhr & Lee Rainie, *E-Reading Rises as Device Ownership Jumps*, PEW RES. CENTER (Jan. 16, 2014), http://www.pewinternet.org/2014/01/16/e-reading-rises-as-device-ownership-jumps/.

35. Michael DeGusta, *Are Smart Phones Spreading Faster than Any Technology in Human History?*, M.I.T. TECH. REV. (May 9, 2012), http://www.technologyreview.com/news/427787/are-smart-phones-spreading-faster-than-any-technology-in-human-history/ (emphasis in original).

36. United States v. Saboonchi, 990 F. Supp. 2d 539, 556 (D. Md. 2014).

37. AARON SMITH ET AL., PEW RESEARCH CTR., U.S. SMARTPHONE USE IN 2015, at 33 (2015), *available at* http://www.pewinternet.org/files/2015/03/PI_Smartphones_0401151.pdf (noting, for example, that ninety-seven percent of smartphone users used text messaging, eighty-nine percent used the internet, eighty-eight percent used email, seventy-five percent used social networking, and sixty percent took pictures or video).

38. *Id.* at 5.

its user and stores that information on the phone, creating an individualized map of daily routines.[39] Many third-party smartphone applications track location information and increasingly condition services on collection of that information.[40]

Border agents likely search the electronic devices of at least several thousand people annually. They searched electronic devices of 4957 people from October 1, 2012 to August 31, 2013[41] and 6671 people during a twenty-month period spanning 2008 to 2010.[42] An electronic device search could include anything from a brief physical inspection to a search of the device's contents to copying the device's contents for the completion of a future forensic examination.[43] The search could also involve retention of the device to enable a search or seizure of the device as evidence of a crime or for civil forfeiture.[44] Department of Homeland Security (DHS) considers electronic devices to be no different from physical containers such as luggage.[45]

A. The Fourth Amendment: Warrant, Probable Cause, and Reasonable Suspicion

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches or seizures."[46] The Amendment establishes a two-part structure

---

39. Molly McHugh, *A Map in Your iPhone Is Tracking You. Here's How to Zap It*, WIRED (Nov. 13, 2015), http://www.wired.com/2015/11/how-to-get-rid-of-the-iphone-map-that-tracks-you/.

40. David Pierce, *Location Is Your Most Critical Data, and Everyone's Watching*, WIRED (Apr. 27, 2015), http://www.wired.com/2015/04/location/ (discussing increased business interest in individual location information, potential benefits to consumers for allowing businesses to track everywhere they go, and privacy tradeoffs).

41. Susan Stellin, *The Border Is a Back Door for U.S. Device Searches*, N.Y. TIMES, Sept. 10, 2013, at B1.

42. *See Government Data Regarding Electronic Device Searches*, ACLU, https://www.aclu.org/national-security/government-data-regarding-electronic-device-searches (last visited Oct. 28, 2015) (summarizing CBP data released pursuant to Freedom of Information Act suit). A 2010 review conducted by CBP's Office of Internal Affairs, Management and Inspection Division, found that CBP did not have a way to provide accurate data on border searches of electronic devices. U.S. DEP'T OF HOMELAND SEC., CIVIL RIGHTS/CIVIL LIBERTIES IMPACT ASSESSMENT: BORDER SEARCHES OF ELECTRONIC DEVICES DECEMBER 29, 2011, at 2, 7 (2011), *available at* http://www.dhs.gov/sites/default/files/publications/Redacted%20Report.pdf (partially redacted).

43. U.S. DEP'T OF HOMELAND SEC., *supra* note 42 at 2.

44. *Id.*

45. *Id.* at 7.

46. U.S. CONST. amend. IV.

for analyzing searches.[47] First, to determine whether the Fourth Amendment applies, courts assess whether the search invades an individual interest protected by the Amendment.[48] Courts generally use the "reasonable expectation of privacy" test to determine whether a particular search implicates an interest protected by the Fourth Amendment.[49] Under this test, an individual must exhibit a subjective expectation of privacy and society must recognize that expectation as reasonable.[50]

Second, the Fourth Amendment requires searches to be "reasonable,"[51] which "generally requires the obtaining of a judicial warrant" supported by probable cause.[52] The policy behind the warrant requirement is to ensure that "the inferences to support a search are 'drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.'"[53] The Supreme Court has repeatedly stated that "searches

---

47. *See* THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION § 1.2, at 3–4 (2d ed. 2014).

48. *See id.* § 1.2.1.2, at 7–10.

49. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); Peter P. Swire, Katz *Is Dead. Long Live* Katz, 102 MICH. L. REV. 904, 904 (2004) (calling *Katz* "the king of Supreme Court surveillance cases"). Some scholars have called for the Court to abandon the reasonable expectation of privacy test. *See, e.g.*, Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1511 (2010) ("The reasonable expectation of privacy test has led to a contentious jurisprudence that is riddled with inconsistency and incoherence."). In place of the *Katz* two-step, Professor Solove urges courts to provide regulation and oversight "whenever a particular government information gathering activity creates problems of reasonable significance." *Id.* at 1514. Under Solove's approach, courts should embrace the broad language of the Fourth Amendment's prohibition against "unreasonable" searches and seizures to protect against "not only invasion of privacy, but also chilling of free speech, free association, freedom of belief, and consumption of ideas." *Id.*

50. *See* Bond v. United States, 529 U.S. 347, 361 (2000) ("Our Fourth Amendment analysis embraces two questions. First, we ask whether the individual, by his conduct, has exhibited an actual expectation of privacy . . . . Second, we inquire whether the individual's expectation of privacy is one that society is prepared to recognize as reasonable." (citations omitted) (internal quotations omitted)).

51. *See* Riley v. California, __ U.S. __, 134 S. Ct. 2473, 2482 (2014) ("[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness.'"(quoting Brigham City v. Stuart, 547 U.S. 398, 403 (2006))).

52. *See id.* (quoting Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995)); Kentucky v. King, 563 U.S. 452, 459 (2011) ("Although the text of the Fourth Amendment does not specify when a search warrant must be obtained, this Court has inferred that a warrant must generally be secured."); *cf.* CLANCY, *supra* note 47, § 11.3, at 571 (discussing the five analytical models the Supreme Court uses to ascertain the reasonableness of a search: "the warrant preference model; the individualized suspicion model; the totality of the circumstances test; the balancing test; and a hybrid model giving dispositive weight to the common law").

53. *Riley*, 134 S. Ct. at 2482 (quoting Johnson v. United States, 333 U.S. 10, 14 (1948)).

conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."[54]

To obtain a warrant, police must establish probable cause by pointing to "specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant th[e] intrusion."[55] The Court has described the probable cause standard as requiring a fair probability that the individual to be searched has committed the crime or that evidence of the crime will be found.[56] Even if the Court finds that a search falls within an exception to the warrant requirement, it may still require that the search satisfy either probable cause[57] or a lesser standard called "reasonable suspicion."[58] To establish reasonable suspicion, law enforcement officers must have a "particularized and objective basis for suspecting the person stopped of criminal activity" based on "the totality of the circumstances."[59] In sum, the Fourth Amendment establishes a

---

54. Arizona v. Gant, 556 U.S. 332, 338 (2009) (quoting *Katz*, 389 U.S. at 357); *see also King*, 563 U.S. at 459. There are a variety of exceptions to the Fourth Amendment probable cause and warrant requirements, including:

> [I]nvestigatory stops, investigatory detentions of property, searches incident to valid arrests, seizures of items in plain view, searches and seizures justified by exigent circumstances, consensual searches, searches of vehicles, searches of containers, inventory searches, border searches, searches at sea, administrative searches, and searches in which the special needs of law enforcement make the probable cause and warrant requirements impracticable.

Warrantless Searches and Seizures, 41 GEO. L.J. ANN. REV. CRIM. PROC. 46 (2012). To obtain a warrant authorizing a search or seizure, the government must demonstrate to a judge or magistrate two elements. First, that there is "probable cause" to believe that a particular individual or group of individuals is engaged in criminal activity. *See, e.g.*, Virginia v. Moore, 553 U.S. 164, 178 (2008); *see also* CLANCY, *supra* note 47, § 11.3.2.1.1, at 577–79. Second, the government must show there is probable cause to believe that the person, place, or thing to be searched has evidence of a crime. *See, e.g.*, United States v. Karo, 468 U.S. 705, 717 (1984). The government must have "reasonably trustworthy information" that is sufficient to "warrant a man of reasonable caution in the belief that an offense has been or is being committed" or that the government will find evidence of a crime in the place to be searched. Brinegar v. United States, 338 U.S. 160, 175–76 (1949) (citations omitted) (internal quotations omitted). Many jurisdictions have made it possible to obtain a warrant quickly, even within five minutes. *See* Missouri v. McNeely, __ U.S. __, 133 S. Ct. 1552, 1573 (2013) (Roberts, C.J., concurring in part and dissenting in part).

55. Terry v. Ohio, 392 U.S. 1, 18 (1968).

56. Safford Unified Sch. Dist. No. 1 v. Redding, 557 U.S. 364, 371 (2009).

57. *See* Ker v. California, 374 U.S. 23, 34–35 (1963).

58. *See* United States v. Arvizu, 534 U.S. 266, 273 (2002); Illinois v. Wardlow, 528 U.S. 119, 123 (2000); United States v. Cortez, 449 U.S. 411, 418 (1981); *Terry*, 392 U.S. at 37; CLANCY, *supra* note 47, § 11.3.2.1.2, at 579.

59. *Cortez*, 449 U.S. at 417–18; *see also Terry*, 392 U.S. at 21 (holding that to justify an intrusion on reasonable suspicion, an officer must be able "to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant [the] intrusion").

baseline standard of a warrant supported by probable cause prior to the search.[60] But, because "the ultimate touchstone of the Fourth Amendment is 'reasonableness,'"[61] the Court has delineated a range of lesser standards for limited exceptions, including probable cause without a warrant, reasonable suspicion, and no suspicion.[62] Finally, under the Fourth Amendment's particularity requirement, all searches—whether pursuant to a warrant or an exception to the warrant requirement—must be "reasonably related in scope to the circumstances which justified the interference in the first place."[63]

B. The Border Search Exception

Under the border search exception, United States officials may conduct "routine" searches and seizures of persons and property at the border without obtaining a warrant or establishing probable cause or reasonable suspicion.[64] The border search exception applies to the international border and its "functional equivalent,"[65] which includes ports of entry[66] and international airports.[67] It covers individuals and

60. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995).

61. Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

62. *See, e.g.*, Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 298–299 (1967) (stating that no search warrant is required under exigent circumstances if probable cause has been met: "The Fourth Amendment does not require police officers to delay in the course of an investigation [by obtaining a warrant] if to do so would gravely endanger their lives or the lives of others"); *Terry*, 392 U.S. at 27 (holding that an officer may search an individual for weapons based on reasonable suspicion even if the officer does not have probable cause or a warrant); United States v. Flores-Montano, 541 U.S. 149, 152–53 (2004) (determining that the disassembly of vehicle gas tank at the border did not require reasonable suspicion, probable cause, or a warrant).

63. New Jersey v. T.L.O., 469 U.S. 325, 341 (1985); *see also* CLANCY, *supra* note 47, § 11.6.1.1, at 637–38.

64. United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985); *see also* CLANCY, *supra* note 47, § 10.2.2, at 491–97; 5 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 10.5(a) (5th ed. 2012 & Supp. 2014). The border search exception is an exception to the baseline warrant requirement, not the Fourth Amendment itself. *See* United States v. Ramsey, 431 U.S. 606, 621 (1977) (holding that the border search exception "is a longstanding, historically recognized exception to the Fourth Amendment's general principle that a warrant be obtained"); United States v. Kim, No. 13-cr-00100-ABJ, 2015 BL 134375, at *22–23 (D.D.C May 8, 2015), *available at* https://cdn.arstechnica.net/wp-content/uploads/2015/05/kimruling.pdf (noting that the Fourth Amendment's reasonableness requirement still applies to border searches).

65. *See* Almeida-Sanchez v. United States, 413 U.S. 266, 272 (1973) ("Whatever the permissible scope of intrusiveness of a routine border search might be, searches of this kind may in certain circumstances take place not only at the border itself, but at its functional equivalents as well.").

66. *See, e.g.*, United States v. Prince, 491 F.2d 655, 659 (5th Cir. 1974) (noting that the port where a ship docks after arriving from a foreign country is the "functional equivalent" of the border (citing *Almeida-Sanchez*, 413 U.S. at 272–73)).

67. *See, e.g.*, United States v. Lawson, 461 F.3d 697, 700 (6th Cir. 2006) (finding Detroit

objects entering or exiting the United States,[68] although courts have offered differing explanations for why the exception applies equally to entrance and exit searches.[69] The historic justification for the border search exception has been the government's right to exclude people or contraband from entering the country.[70] This interest allows the government wide latitude to conduct searches that the Fourth Amendment would not allow in other contexts.[71]

The Supreme Court has outlined the contours of the border search exception in three main cases: *United States v. Ramsey*,[72] *United States v. Montoya de Hernandez*,[73] and *United States v. Flores-Montano*.[74] In *Ramsey*, the Court established that border searches of people and property generally do not require a warrant or probable cause.[75] The

---

International Airport the "functional equivalent" of the border for flights arriving from foreign countries); United States v. Klein, 592 F.2d 909, 911 n.1 (5th Cir. 1979) (finding that an airport where an international flight lands qualifies as the "functional equivalent" of the border). Passengers on domestic flights are not searched pursuant to the border search exception. Rather, the administrative search exception—reserved for searches unrelated to law enforcement—is used to justify routine searches of individuals and their effects on domestic flights. *See* United States v. Davis, 482 F.2d 893, 908–12 (9th Cir. 1973).

68. *See, e.g.*, United States v. Berisha, 925 F.2d 791, 795 (5th Cir. 1991) (holding that routine stops and searches for currency of travelers exiting the United States fall within the border search exception).

69. Larry Cunningham, *The Border Search Exception as Applied to Exit and Export Searches: A Global Conceptualization*, 26 QUINNIPIAC L. REV. 1, 15–29, app. at 40–55 (2007).

70. United States v. 12 200-Ft. Reels of Super 8MM Film (*12 200-Ft. Reels of Film*), 413 U.S. 123, 125 (1973) ("The Constitution gives Congress broad, comprehensive powers '[t]o regulate Commerce with foreign Nations.' Historically such broad powers have been necessary to prevent smuggling and to prevent prohibited articles from entry." (alteration in original) (quoting U.S. CONST. art. I, § 8, cl. 3)).

71. *See id.* ("Import restrictions and searches of persons or packages at the national borders rest on different considerations and different rules of constitutional law from domestic regulations."); Carroll v. United States, 267 U.S. 132, 153–54 (1925) ("Travelers 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."). The first Congress granted customs officials "full power and authority" to search ships entering United States ports without a warrant if officials had "reason to suspect any goods, ware or merchandise subject to duty shall be concealed." Act of July 31, 1789, ch. 5, §§ 23–24, 1 Stat. 29, 43. Courts have interpreted the "reason to suspect" language of the statute as requiring the same standard as "reasonable suspicion." *See, e.g.*, United States v. Ramsey, 431 U.S. 606, 612–13 (1977) ("The 'reasonable cause to suspect' test adopted by the [current] statute [derived from the 1789 Act] is, we think, a practical test which imposes a less stringent requirement than that of 'probable cause' imposed by the Fourth Amendment as a requirement for the issuance of warrants." (citing Terry v. Ohio, 392 U.S. 1, 8 (1968))).

72. 431 U.S. 606 (1977).

73. 473 U.S. 531 (1985).

74. 541 U.S. 149 (2004).

75. *Ramsey*, 431 U.S. at 619. The Court mentioned the border search exception in dicta in earlier

Court upheld a customs official's search of several envelopes mailed from Thailand to the United States.[76] The officer had reasonable suspicion that the envelopes contained merchandise or contraband other than mere correspondence, and discovered heroin.[77] The Court declined to require a warrant or probable cause for the search in light of the government's heightened interests in prohibiting contraband from entering the country.[78] The Court explained that border searches "are reasonable simply by virtue of the fact that they occur at the border," reflecting the "long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country."[79]

Despite this somewhat sweeping language, *Ramsey* did not establish that government officials may conduct any kind of border search without suspicion of criminal activity.[80] Rather, the Court found that the customs agent had reasonable suspicion of a violation of customs law; the Court did not need to decide whether the Fourth Amendment would allow a suspicionless search of an envelope.[81] The Court concluded it would make little sense to carve out special protection for envelopes that enter the United States by mail when, as the petitioner conceded, officials could warrantlessly search the same envelopes if a traveler physically carried them into the country.[82]

Perhaps most important, nothing in *Ramsey* suggests border agents may search or read the *content* of correspondence without a warrant. The

---

decisions but did not expressly rule on it until *Ramsey*. *See 12 200-Ft. Reels of Film*, 413 U.S. at 125; Almeida-Sanchez v. United States, 413 U.S. 266, 272 (1973); United States v. Thirty-Seven Photographs, 402 U.S. 363, 376 (1971); *Carroll*, 267 U.S. at 154 ("Travelers 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."); Boyd v. United States, 116 U.S. 616, 622 (1886).

76. *Ramsey*, 431 U.S. at 607–08.

77. *Id.* at 609.

78. *Id.* at 619.

79. *Id.* at 620 ("The border-search exception is grounded in the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country."); *see also Thirty-Seven Photographs*, 402 U.S. at 376 (noting that the border search "is an old practice and is intimately associated with excluding illegal articles from the country").

80. *See Ramsey*, 431 U.S. at 625 (Powell, J., concurring).

81. *Id.* at 614 (majority opinion). The Court found that reasonable suspicion of a customs violation had been established on the following facts: the envelopes were "bulky" and weighed "three to six times the normal weight of an airmail letter"; they were from Thailand, "a known source of narcotics"; they bore addresses of four different locations, apparently typed with the same typewriter; and, from physical touch, they felt like they contained more than "just plain paper." *Id.* at 609.

82. *Id.* at 620.

Court emphasized that "[a]pplicable postal regulations flatly prohibit, under all circumstances, the reading of correspondence absent a search warrant," and rejected the dissent's concerns about chilled speech on that basis.[83] Justice Powell wrote a concurring opinion to underscore his belief that those limits were sufficient to protect the First and Fourth Amendment rights at stake in the border context.[84]

The rule under *Ramsey* is that officials may conduct routine border searches without a warrant or probable cause when those searches are tethered to the government's interest in examining persons and property seeking entrance to the United States.[85] The Court did not sanction suspicionless searches of mailed correspondence.[86] The Court also expressly reserved the question of "whether, and under what circumstances, a border search might be deemed 'unreasonable' because of the particularly offensive manner in which it is carried out."[87]

C. "Routine" and "Nonroutine" Border Searches

The Supreme Court distinguished between "routine" and "nonroutine" border searches and seizures in *United States v. Montoya de Hernandez*.[88] The Court explained that, under *Ramsey*, "[r]outine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant,"[89] but that the Court had "not previously decided what level of suspicion would justify a seizure of an incoming traveler for purposes other than a routine border search."[90]

Customs officials detained Montoya de Hernandez, who was traveling on a direct flight from Bogota, Colombia, to Los Angeles, California on suspicion that she was smuggling drugs—specifically, that she had swallowed balloons of cocaine.[91] The facts of the case "clearly supported" the customs agents' reasonable suspicion that Montoya de Hernandez was a cocaine smuggler.[92] Montoya de Hernandez claimed

83. *Id.* at 623.

84. *See id.* at 625 (Powell, J., concurring).

85. *Id.* at 616 (majority opinion).

86. *Id.* at 623.

87. *Id.* at 618 n.13.

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

89. *Id.* at 538.

90. *Id.* at 540.

91. *Id.* at 532–36.

92. *Id.* at 542. She had made eight recent trips to Miami and Los Angeles, but had no family or friends in the United States and no hotel reservations, despite arriving shortly after midnight. She

she was pregnant and agreed to take a pregnancy test.[93] She declined to be x-rayed, and the customs inspectors informed her that they would detain her until she either agreed to an x-ray or produced a monitored bowel movement that would confirm or deny their suspicions.[94] After sixteen hours of detention, border officials obtained a court order to conduct a rectal examination, which produced balloons of cocaine.[95]

The Court held that the customs officials' reasonable suspicion that Montoya de Hernandez was smuggling drugs in her alimentary canal was sufficient to justify her temporary detention.[96] The Court explained that the reasonable suspicion standard "fits well into the situations involving alimentary canal smuggling at the border," where the government has significant interests in preventing drug smuggling but would "rarely possess probable cause," at least in part because this kind of smuggling "gives no external signs."[97] The standard "effects a needed balance between private and public interests when law enforcement officials must make a limited intrusion on less than probable cause."[98]

As in *Ramsey*, the Court characterized the government's interests at the border in broad terms, noting that customs and immigration officials are charged with protecting the country from individuals who would bring in anything harmful, whether in the form of disease or contraband.[99] But the Court's holding was narrow and limited in important respects.[100] First, the Court reiterated that a border search must be "reasonably related in scope to the circumstances which justified it initially."[101] Second, the Court found that reasonable suspicion justified

---

was carrying $5000 in cash, mostly in $50 bills, but had no billfold; although she claimed she was planning to purchase merchandise for her husband's store, she had no appointments with vendors. She could not recall how she purchased her airline ticket. A female customs inspector conducted a pat down and strip search in a private area, finding that Montoya de Hernandez was wearing two pairs of underwear and a paper towel lining her crotch. *Id.* at 533–34.

93. *Id.* at 534.

94. *Id.* at 534–35.

95. *Id.* at 535–36. Over four days, Montoya de Hernandez eventually passed eighty-eight balloons containing 528 grams of cocaine. *Id.* at 536.

96. *Id.* at 541.

97. *Id.*

98. *Id.*

99. *Id.* at 544.

100. *Id.* ("We hold that the detention of a traveler at the border, beyond the scope of a routine customs search and inspection, is justified at its inception if customs agents, considering all the facts surrounding the traveler and her trip, reasonably suspect that the traveler is smuggling contraband in her alimentary canal.").

101. *Id.* at 542. In assessing whether Montoya de Hernandez's prolonged incommunicado detention was "reasonably related in scope to the circumstances which justified it initially," the

Montoya de Hernandez's initial temporary detention, but not necessarily a body cavity search.[102] Rather, the Court left open the possibility that a body cavity search would be so intrusive as to require evidence establishing reasonable suspicion or a higher standard, such as probable cause or a warrant.[103] The Court noted: "[W]e suggest no view on what level of suspicion, if any, is required for nonroutine border searches such as strip, body cavity, or involuntary x-ray searches."[104]

The Supreme Court's last major statement on border searches came in *United States v. Flores-Montano*,[105] in which it held that a search involving the disassembly of an automobile gasoline tank did not require reasonable suspicion.[106] The Court rejected arguments that the defendant had any privacy interest in his gas tank protected by the Fourth Amendment,[107] or any right to prevent a potentially destructive search of the tank.[108] The Court made it clear that the search of a gas tank was not the kind of "nonroutine" or highly intrusive search contemplated by *Montoya de Hernandez*.[109] The Court explained:

> [T]he reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person—dignity and privacy interests of the person being searched—simply do not carry over to vehicles. Complex balancing tests to determine what is a "routine" search of a vehicle, as opposed to a more "intrusive" search of a person, have no place in border searches of vehicles.[110]

The Court qualified this statement by leaving open the possibility that a search could be "so destructive" of one's property as to warrant similar

---

Court found it significant that Montoya de Hernandez refused to submit to an x-ray. *Id.* at 542–43. "Respondent alone was responsible for much of the duration and discomfort of the seizure." *Id.* at 543.

102. *Id.* at 541 & n.4.

103. *Id.* at 541.

104. *Id.* at 541 n.4. The Ninth Circuit has held that reasonable suspicion is required for a strip search at the border. United States v. Chase, 503 F.2d 571, 574 (9th Cir. 1974).

105. 541 U.S. 149 (2004).

106. *Id.* at 155–56.

107. *Id.* at 154 ("It is difficult to imagine how the search of a gas tank, which should be solely a repository for fuel, could be more of an invasion of privacy than the search of the automobile's passenger compartment.").

108. *Id.* at 155–56. The Court left open the possibility that a search could be "so destructive" of one's property as to warrant a requirement of reasonable suspicion: "While it may be true that some searches of property are so destructive as to require a different result, this was not one of them." *Id.*

109. *Id.* at 152.

110. *Id.*

protection to that of an "intrusive" search of a person.[111]

The sum of *Ramsey*, *Montoya de Hernandez*, and *Flores-Montano* leave government officials with relatively wide latitude to conduct routine border searches and seizures of persons and property without suspicion of wrongdoing.[112] The government has significant interests in preventing the entrance of unwanted people and contraband, and individuals crossing the border have a reduced expectation of privacy in their person and effects.[113] Nevertheless, the Court has insisted that the Fourth Amendment applies to border searches. It has also indicated that searches that are particularly destructive to property or highly intrusive to a person likely warrant a heightened standard, and reserved the question as to whether such searches would require reasonable suspicion, probable cause, or a warrant.[114]

One lingering issue is the distinction between "routine" and "nonroutine" border searches. The Court has yet to define what searches would be "nonroutine," or what level of process it would impose for such searches.[115] Nevertheless, lower federal courts have found the "intrusiveness" of the search—the extent to which the search invades an individual's privacy—is what distinguishes a "routine" from a "nonroutine" border search.[116] Courts have considered personal searches that involve "some level of indignity or intrusiveness," but fall short of a

---

111. *Id.* at 155–56. Before *Flores-Montano*, federal circuit courts defined destructive property searches, including drilling into a vehicle or package, as nonroutine border searches requiring reasonable suspicion. *See, e.g.*, United States v. Rivas, 157 F.3d 364, 367 (5th Cir. 1998) (drilling into the body of a trailer); United States v. Robles, 45 F.3d 1, 5 (1st Cir. 1995) (drilling into a metal cylinder in a wooden crate); United States v. Carreon, 872 F.2d 1436, 1440 (10th Cir. 1989) (holding reasonable suspicion justified extension of routine vehicle search to include drilling a hole in a camper wall). After *Flores-Montano*, courts have been more reluctant to scrutinize such property searches. *E.g.*, United States v. Cortez-Rocha, 394 F.3d 1115, 1125 (9th Cir. 2005) (noting that cutting open spare tire in context of border search did not require reasonable suspicion).

112. United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985) ("Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant, and first-class mail may be opened without a warrant on less than probable cause." (footnote omitted) (citation omitted)).

113. *Flores-Montano*, 541 U.S. at 154 ("[O]n many occasions, we have noted that the expectation of privacy is less at the border than it is in the interior.").

114. *Id.* at 155–56.

115. *See, e.g.*, United States v. Cotterman, 709 F.3d 952, 963 (9th Cir. 2013) ("The Court has never defined the precise dimensions of a reasonable border search, instead pointing to the necessity of a case-by-case analysis.").

116. *See* United States v. Irving, 452 F.3d 110, 123 (2d Cir. 2006) ("[T]he level of intrusion into a person's privacy is what determines whether a border search is routine."). *But see* United States v. Vega-Barvo, 729 F.2d 1341, 1346 (11th Cir. 1984) (holding that the "personal indignity suffered by the individual searched controls the level of suspicion required to make the search reasonable").

strip or cavity search, to be routine.[117] The First Circuit has listed a number of factors as relevant to deciding whether a search is routine or nonroutine.[118]

On this distinction, lower courts have found searches of an individual's outer clothing, personal effects, purse, and wallet[119] all to be routine in the border context. As one federal district court explained, "pat-downs, pocket-dumps, and even searches that require moving or adjusting clothing without disrobing, and also may include scanning, opening, and rifling through the contents of bags or other closed containers" are all routine kinds of searches.[120] Examples of nonroutine searches requiring reasonable suspicion include strip searches,[121] alimentary canal searches,[122] x-rays,[123] and removal of an artificial limb.[124] In practice, at least in reported cases, the government has demonstrated significant evidence before conducting such intrusive body searches: "It is fair to say that most of the reported cases upholding body cavity border searches have in fact involved rather strong evidence that smuggled goods were being carried in a body cavity."[125]

---

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

118. United States v. Braks, 842 F.2d 509, 512 (1st Cir. 1988). Factors include:

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

Id. (footnotes omitted).

119. United States v. Johnson, 991 F.2d 1287, 1291–92 (7th Cir. 1993).

120. *Saboonchi*, 990 F. Supp. 2d at 549.

121. United States v. Adekunle, 980 F.2d 985, 987–88 (5th Cir. 1992); United States v. Asbury, 586 F.2d 973, 975–76 (2d Cir. 1978); Henderson v. United States, 390 F.2d 805, 809 (9th Cir. 1967); *see also* United States v. Palmer, 575 F.2d 721, 723 (9th Cir. 1978) (requiring a woman to "lift her dress so that [her] girdle could be observed").

122. *See* Rivas v. United States, 368 F.2d 703, 710 (9th Cir. 1966).

123. United States v. Vega-Barvo, 729 F.2d 1341, 1349 (11th Cir. 1984). The Supreme Court and the Fourth Circuit have also assumed that an x-ray search is nonroutine. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 541 n.4 (1985); United States v. Aguebor, No. 98-4258, 1999 WL 5110 (4th Cir. Jan. 4, 1999).

124. United States v. Sanders, 663 F.2d 1, 3 (2d Cir. 1981).

125. LAFAVE, *supra* note 64, § 10.5(e), at 255.

II. DIGITAL BORDER SEARCHES

ICE and CBP have authorized border officers to search, copy, and retain digital information contained on, or accessible through, electronic devices at the border without individualized suspicion of criminal activity.[126] Defendants have challenged these searches as unreasonable under the Fourth Amendment. In particular, defendants have argued that digital border searches are nonroutine and require reasonable suspicion.[127] This Part discusses major developments in the digital border search case law.

Part II.A discusses the first wave of major federal appellate cases. Under the initial prevailing approach, courts generally treated computer searches as routine and not requiring reasonable suspicion.[128] In two paradigmatic cases—the Fourth Circuit's decision in *United States v. Ickes*[129] and the Ninth Circuit's decision in *United States v. Arnold*—courts reached this conclusion by analogizing a search for digital information on a computer to a search for physical items held in a physical container, such as luggage or the glove compartment of a car.[130]

Part II.B discusses a second major doctrinal development, where two federal courts have concluded that a "forensic" digital border search is nonroutine and requires reasonable suspicion.[131] The Ninth Circuit, in *United States v. Cotterman*, and the District of Maryland, in *United*

126. ICE DIRECTIVE, *supra* note 2, § 6.1, at 2; CBP DIRECTIVE, *supra* note 2, § 5.1.2, at 3. Both policies permit indefinite detention of data that pertains to immigration, customs, or other law enforcement matters. U.S. DEP'T OF HOMELAND SEC., *supra* note 42, at 15; ICE DIRECTIVE, *supra* note 2, § 8.5(1), at 7; CBP DIRECTIVE, *supra* note 2, § 5.4.1.2, at 7. The policies also permit retention of all devices and data for a reasonable time to conduct a thorough search. This is generally five days under the CBP policy and thirty days under the ICE policy, but both allow extensions of time with supervisory approval or extenuating circumstances. ICE DIRECTIVE, *supra* note 2, § 8.3(1), at 4–5; CBP DIRECTIVE, *supra* note 2, § 5.3.1, at 4.

127. *See generally infra* Part II.A–B.

128. *See, e.g.*, United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008) (holding that the Fourth Amendment does not protect electronic devices, including computers and cell phones, from warrantless and suspicionless searches in border context); United States v. Linarez-Delgado, 259 F. App'x 506, 508 (3d Cir. 2007) (no reasonable suspicion required for a routine border search of "[d]ata storage media and electronic equipment, such as films, computer devices, and videotapes"); United States v. Ickes, 393 F.3d 501, 504 (4th Cir. 2005) (no suspicion required for computer search at the border); Abidor v. Napolitano, 990 F. Supp. 2d 260, 277–78 (E.D.N.Y. 2013) (dismissing the lawsuit for lack of standing, but nevertheless concluding that reasonable suspicion was not required for a laptop search); United States v. Bunty, 617 F. Supp. 2d 359, 365 (E.D. Pa. 2008) (no reasonable suspicion required to search through computer disks).

129. 393 F.3d 501 (4th Cir. 2005).

130. *See infra* notes 166–75 and accompanying text.

131. United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013); United States v. Saboonchi, 990 F. Supp. 2d 536, 539 (D. Md. 2014).

States v. Saboonchi, moved away from the "container" analogy and recognized distinct Fourth Amendment interests implicated by extensive searches of digital information.[132] Nevertheless, both courts agreed that border agents may conduct manual digital border searches of electronic devices without reasonable suspicion, thereby affirming a core holding common to *Ickes* and *Arnold*.[133]

Courts have generally focused on whether reasonable suspicion is required for the search. In almost all cases federal courts have found that government agents had established reasonable suspicion.[134] Some courts have reached the question of whether reasonable suspicion is required, even while finding that it has been met.[135] Others have declined to reach the question either because they found that the search was routine[136] or to avoid reaching a constitutional question that was not necessary for the disposition of the case.[137] As a practical matter, the federal government has consistently argued that it does not need reasonable suspicion to conduct a digital border search, no matter how intrusive.[138]

---

132. *See infra* Part II.B.

133. *Cotterman*, 709 F.3d at 966–67; *Saboonchi*, 990 F. Supp. 2d at 546.

134. *See Cotterman*, 709 F.3d at 970 (border agents had reasonable suspicion); United States v. Ickes, 393 F.3d 501, 503–05 (4th Cir. 2005) (suggesting that reasonable suspicion had been met but nevertheless holding that no suspicion was required); United States v. Roberts, 274 F.3d 1007, 1014 (5th Cir. 2001) (customs agents had reasonable suspicion); United States v Hassanshahi, 75 F. Supp. 3d 101, 119 (D.D.C. 2014) (same); *Saboonchi*, 990 F. Supp. 2d at 571 (same); Abidor v. Napolitano, 990 F. Supp. 2d 260, 282 (E.D.N.Y. 2013) (finding reasonable suspicion). *But see* United States v. Stewart, 729 F.3d 517, 524 (6th Cir. 2013) (initial computer search was routine, not requiring reasonable suspicion).

135. *See Cotterman*, 709 F.3d at 968 (reasonable suspicion satisfied); *Abidor*, 990 F. Supp. 2d at 282 (same).

136. *See* United States v. Linarez-Delgado, 259 F. App'x 506, 508 (3d Cir. 2007). Courts have also considered arguments that conducting a computer search away from the border is an "extended border search"—a search that occurs after an individual has been cleared for entry and regained a reasonable expectation of privacy. Extended border searches require reasonable suspicion of criminal activity. But, where a computer has not been cleared for entry, as in most cases, courts have rejected arguments that a subsequent offsite search is an extended border search. *E.g.*, *Stewart*, 729 F.3d at 524–26 (sending laptop off site to conduct a search, but not a forensic examination, was a continuation of a routine border search and not an extended border search requiring reasonable suspicion).

137. *See* United States v. Irving, 452 F.3d 110, 124 (2d Cir. 2006) (finding reasonable suspicion met and declining to determine whether search of computer diskettes and undeveloped film required reasonable suspicion); *Hassanshahi*, 75 F. Supp. 3d at 119.

138. *See, e.g.*, *Cotterman*, 709 F.3d at 959 ("[H]aving failed to obtain a favorable ruling on that ground, the government did not challenge on appeal the conclusion that there was no reasonable suspicion. Rather, it sought a broad ruling that no suspicion of any kind was required."); United States v. Kim, No. 13-cr-00100-ABJ, 2015 BL 134375, at *1 (D.D.C. May 8, 2015), *available at* https://cdn.arstechnica.net/wp-content/uploads/2015/05/kimruling.pdf; *see also Saboonchi*, 990 F. Supp. 2d at 540 (government arguing forensic digital border search was routine).

At the outset, it is useful to note that border searches of electronic devices can take at least three forms. This Comment draws descriptive categories based on examples from DHS policies and case law: (1) a physical device search (which is not the primary subject of this Comment) and two kinds of digital searches, (2) a manual digital search and (3) a forensic digital search. Border officials may digitally search a wide range of devices: "any devices that may contain information, such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players, and any other electronic or digital devices."[139]

In a physical device search, a border officer examines physical aspects of the device, not the information stored on it.[140] For example, the agent might ask an individual to turn on a cell phone, camera, or computer to confirm that the device is what it appears to be.[141] This may also involve physically opening the device to determine whether it contains anything out of the ordinary.[142] In any case, the agent does not examine data stored on or accessed via the device, and the overall purpose of the search is to find physical evidence that may be contained inside the device or confirm that the device is what it appears to be.

In a manual digital search, an officer searches digital information contained on or accessible through the device.[143] This could be a relatively superficial search—scrolling through contacts or recent calls on a smartphone, or opening up a desktop folder to browse the names of files.[144] But it could also include a relatively extensive examination of digital information, depending in large part on how much time the officer has to search.[145]

---

139. CBP DIRECTIVE, *supra* note 2, § 3.2, at 2.

140. *See id.* § 3.4, at 2 (distinguishing between searches for digital information and turning a device on or determining whether a device contains physical contraband).

141. *See, e.g.*, United States v. Arnold, 533 F.3d 1003, 1005 (9th Cir. 2008) (CBP officer "instructed Arnold to turn on the computer so she could see if it was functioning").

142. *See, e.g.*, United States v. Molina–Gómez, 781 F.3d 13, 17 (1st Cir. 2015) (discussing a search where a border official disassembled laptop computer and Playstation and discovered black bags containing heroin hidden inside); *Abidor*, 990 F. Supp. 2d at 268 (Abidor alleged that his laptop and external hard drive had been physically opened in addition to being searched).

143. *See, e.g.*, *Arnold*, 533 F.3d at 1005 ("When the computer had booted up, its desktop displayed numerous icons and folders. Two folders were entitled 'Kodak Pictures' and one was entitled 'Kodak Memories.' [CBP officers] Peng and Roberts clicked on the Kodak folders, opened the files, and viewed the photos on Arnold's computer including one that depicted two nude women.").

144. *See id.*

145. For example, in *Arnold*, after the initial search turned up suspicious images, border officers detained Arnold for several hours and thoroughly searched his computer. *Id.* In *United States v.*

Finally, a forensic digital search is similar to a digital border search in that the goal is to identify information stored on the device, but it has several distinct technical aspects that make it potentially more exhaustive.[146] In most cases, an officer first confiscates the electronic device. A computer expert then makes an exact copy of the device's hard drive and uses sophisticated software to exhaustively search all data on the device, including ostensibly deleted files.[147] The search can take days, weeks, or months, depending on the amount of data.[148]

It is relatively easy to distinguish between a physical device search and either kind of digital search. The physical search examines only physical aspects of the device, whereas a digital search is a search of, and for, information. It is more difficult to differentiate a manual digital search from a forensic digital search, because both involve informational searches, but courts have generally looked to the method of the search to draw the distinction. For example, in *United States v. Saboonchi*, the court identified three aspects of the process that make a search "forensic."[149] These aspects include creating an exact copy of the

---

Kim, No. 13-cr-00100-ABJ, 2015 BL 134375, at *19–20 (D.D.C. May 8, 2015), *available at* https://cdn.arstechnica.net/wp-content/uploads/2015/05/kimruling.pdf, the government argued that the search at issue was not "forensic" because a person with unlimited time could locate the same documents. *See also* United States v. Saboonchi, 990 F. Supp. 2d 536, 547 (D. Md. 2014) (acknowledging that digital border searches that are not "forensic" may nevertheless be "deeply probing and . . . invasive").

146. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 537–47 (2005) (discussing technical details and practices involved in computer forensics).

147. *E.g.*, United States v. Cotterman, 709 F.3d 952, 958 (9th Cir. 2013). In *Cotterman*:

> The agents . . . retained the Cottermans' laptops and a digital camera. Agent Brisbine drove almost 170 miles . . . to the ICE office in Tucson, Arizona, where he delivered both laptops and one of the three digital cameras to ICE Senior Special Agent & Computer Forensic Examiner John Owen. Agent Owen began his examination on Saturday, the following day. He used a forensic program to copy the hard drives of the electronic devices. . . . Agent Owen then used forensic software that often must run for several hours to examine copies of the laptop hard drives. He began his personal examination of the laptops on Sunday. That evening, Agent Owen found seventy-five images of child pornography within the unallocated space of Cotterman's laptop.

Id. (footnotes omitted). "[U]nallocated space" contains deleted data that has yet to be overwritten with new data and can only be accessed with forensic software. *Id.*

148. *Saboonchi*, 990 F. Supp. 2d at 561 ("In a forensic search of electronic storage, a bitstream copy is created and then is searched by an expert using highly specialized analytical software—often over the course of several days, weeks, or months—to locate specific files or file types, recover hidden, deleted, or encrypted data, and analyze the structure of files and of a drive."); *Kim*, 2015 BL 134375, at *15 (DHS special agent stated in affidavit that the "identification and extraction process . . . may take weeks or months" (alteration in original)); Kerr, *supra* note 146, at 544 ("[T]he analyst may spend several weeks or even months analyzing a single hard drive.").

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

device's hard drive;[150] using software that provides access to all information on a device, including previously deleted files;[151] and using software that provides access to location information and other "metadata."[152] But even if courts can distinguish between manual and forensic digital searches based on technical attributes, the amount and kind of information that each search can reveal may be more dependent on nontechnical aspects of the search—especially time—than technical aspects.[153]

A. Digital Border Search 1.0: Digital Border Searches Are Routine and Do Not Require Reasonable Suspicion

Two federal appellate decisions illustrate the first major doctrinal development with respect to digital border searches: the Fourth Circuit's decision in *United States v. Ickes* and the Ninth Circuit's decision in *United States v. Arnold*.

In *Ickes*, the Fourth Circuit held that a manual digital border search of Ickes's computer was routine and that border agents did not have to establish any level of suspicion before executing it.[154] The court treated computer files as indistinguishable from any other "cargo" subject to routine search and inspection at the border.[155] The court rejected Ickes's argument that the First Amendment granted special protection to digital information because it is expressive.[156] Such logic "would create a sanctuary at the border for all expressive material—even for terrorist plans."[157] The court also expressed skepticism that its decision would result in widespread suspicionless digital searches because "[c]ustoms agents have neither the time nor the resources to search the contents of every computer."[158]

Although it declined to do so, the *Ickes* court likely could have found that border officials satisfied reasonable suspicion for the search of his computer.[159] The court acknowledged that Ickes raised suspicion through

150. *Id.* at 564–66.

151. *Id.* at 566–68.

152. *Id.* at 568–69.

153. *See Kim*, 2015 BL 134375, at *19–20.

154. United States v. Ickes, 393 F.3d 501, 505–06 (2005).

155. *Id.* at 504.

156. *Id.* at 506.

157. *Id.*

158. *Id.* at 506–07.

159. *See* United States v. Saboonchi, 990 F. Supp. 2d 536, 546 (D. Md. 2014) (noting that the officers in *Ickes* "likely had reasonable suspicion before they viewed the contents of the disks").

his conduct and possessions, which "suggest[ed] the need to search further," but nevertheless explained that no suspicion was required for the search.[160] Deference to the discretion of border officials, the court said, is the "essence" of the border search exception, which requires "reliance upon the trained observations and judgments of customs officials, rather than upon constitutional requirements" applied in different contexts.[161]

In *Arnold*, the Ninth Circuit also held that digital border searches do not require reasonable suspicion.[162] Arnold was stopped at customs at Los Angeles International Airport after a trip to the Philippines.[163] Border officials asked Arnold to turn on his computer and briefly examined two desktop folders labeled "Kodak Pictures" and "Kodak Memories," one of which revealed a photo of nude women.[164] The border agent called in supervisors who searched his laptop further over several hours, finding numerous images they believed depicted child pornography.[165]

As in *Ickes*, the court premised its holding on the concept that a search of a computer is no different than a search of any other item of personal property.[166] The court found that Arnold "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."[167] The court also

---

Ickes was traveling into the United States from Canada. He told the first border agent that he was on vacation, but his van appeared to hold everything he owned, so a second agent began a cursory inspection. The second agent found a video camera, which contained coverage of a tennis match that focused "excessively on a young ball boy." *Ickes*, 393 F.3d at 502. The agents searched the van and found marijuana seeds and pipes and a copy of a warrant for Ickes's arrest, as well as a computer and several albums containing what appeared to be child pornography. *Id.* at 503.

160. *Ickes*, 393 F.3d at 507.

161. *Id.* In other cases where law enforcement possessed reasonable suspicion of criminal activity prior to a digital border search, courts have generally declined to decide whether the Fourth Amendment permits a suspicionless digital border search. *See, e.g.*, United States v. Irving, 452 F.3d 110, 124 (2d Cir. 2006) ("A border search is valid under the Fourth Amendment, even if non-routine, if it is supported by reasonable suspicion."); *see also* United States v. Roberts, 274 F.3d 1007, 1014 (5th Cir. 2001) (assuming, but not deciding, that a search of a laptop and computer disks is nonroutine, and expressly avoiding the question in order to decide a constitutional question on the narrowest grounds possible).

162. United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008).

163. *Id.* at 1005.

164. *Id.*

165. *Id.*

166. *Id.* at 1008.

167. *Id.* at 1009. The court reasoned that, for border searches, "the Supreme Court has refused to draw distinctions between containers of information and contraband with respect to their quality or

interpreted *Flores-Montano* to create a categorical rule for border searches of physical property, including laptops.[168] Under this reading, border searches of any item of personal property do not implicate privacy or dignity interests.[169]

Concluding that computers are no different from other personal property allowed the court to draw two other conclusions. First, the court compared Arnold's laptop to the gas tank of the car in *Flores-Montano*,[170] where the Supreme Court held that dismantling a gas tank did not require reasonable suspicion but suggested that a particularly destructive search of personal property might.[171] Similarly, the Ninth Circuit reasoned that the search of Arnold's computer would have to have caused significant physical damage to the computer to trigger the reasonable suspicion requirement, but Arnold had made no such claim.[172]

Second, the court analogized the search of the digital information on Arnold's computer to a search of physical items in a closed container such as luggage or a purse or wallet.[173] The court cited *California v. Acevedo*,[174] where the Supreme Court held that the Fourth Amendment permits police to "look[] inside a closed container" when already properly searching a car.[175] The Ninth Circuit concluded that searching a laptop was akin to searching a container and could not be "particularly offensive" to Arnold simply because it could reveal far more information than a search of virtually any other physical container.[176]

---

nature for purposes of determining the appropriate level of Fourth Amendment protection." *Id.* DHS has analogized computers and cell phones to physical containers. *See, e.g.*, U.S. DEP'T OF HOMELAND SEC., *supra* note 42, at 6 ("[Electronic] devices are one of many types of items or containers that may be searched, usually during secondary inspection.").

168. *Arnold*, 533 F.3d at 1008 ("The Supreme Court's analysis [in *Flores-Montano*] determining what protection to give a vehicle was not based on the unique characteristics of vehicles with respect to other property, but was based on the fact that a vehicle, as a piece of property, simply does not implicate the same 'dignity and privacy' concerns as 'highly intrusive searches of the person.'" (quoting United States v. Flores-Montano, 541 U.S. 149, 152 (2004))).

169. *Id.*

170. *Id.* at 1008–09.

171. *Flores-Montano*, 541 U.S. at 155–56.

172. *Arnold*, 533 F.3d at 1009.

173. *Id.* at 1009–10.

174. 500 U.S. 565 (1991).

175. *Id.* at 576.

176. *Arnold*, 533 F.3d at 1009–10. The court also rejected Arnold's argument that a search of a laptop was analogous to a search of a home because of a laptop's storage capacity. *Id.*

B. Digital Border Search 2.0: Forensic Digital Border Searches of Electronic Devices Are Nonroutine and Require Reasonable Suspicion

The principles behind *Arnold* and *Ickes* have come under challenge, particularly in cases involving forensic digital searches at the border. Two recent cases—*United States v. Cotterman* and *United States v. Saboonchi*—show the emergence of a new and competing doctrine on digital border searches that embraces parts of *Arnold* and *Ickes* while repudiating others.

1. United States v. Cotterman

In *Cotterman*, the Ninth Circuit held that a forensic digital border search is nonroutine and requires reasonable suspicion.[177] Sitting en banc, the court concluded that "the comprehensive and intrusive nature of a forensic examination . . . trigger[s] the requirement of reasonable suspicion."[178] The majority explained that the "painstaking analysis" involved in the forensic examination, which included copying and searching Cotterman's hard drive in its entirety, including ostensibly deleted files, "is akin to reading a diary line by line looking for mention of criminal activity—plus looking at everything the writer may have erased."[179]

The court emphasized how the technological capabilities of modern

177. United States v. Cotterman, 709 F.3d 952, 968 (9th Cir. 2013).

178. *Id.* at 962. The district court found that the border agents failed to establish reasonable suspicion and granted Cotterman's motion to suppress. *Id.* at 959. The Ninth Circuit found that border officials had reasonable suspicion and reversed. *Id.* at 957. The Ninth Circuit's reversal of that finding was based on five factors. First, Cotterman and his wife were returning from Mexico, "a country associated with sex tourism." *Id.* at 968–69. Second, at primary inspection the Treasury Enforcement Communication System (TECS), a database used by DHS to track individuals suspected of criminal activity, indicated that Cotterman was convicted of child molestation in 1992 and may be involved in child sex tourism. *Id.* at 957. Third, Cotterman and his wife were carrying a variety of electronic equipment: two computers and three digital cameras. *Id.* Fourth, Cotterman traveled frequently. *Id.* at 969. Fifth, Cotterman protected certain files with password protection, which could be used to further the possession of child pornography. *Id.* Judge Milan Smith, writing in dissent, criticized the majority for finding reasonable suspicion on these "weak facts," which he found fell "woefully short." *Id.* at 982, 990–94 (Smith, J., dissenting). At least one other court has questioned whether being on the TECS list itself supports a finding of reasonable suspicion for a search. *See* United States v. Laich, No. 08-20089, 2010 WL 259041, at *4 (E.D. Mich. Jan. 20, 2010) (finding the fact that Laich was on the TECS list "unpersuasive, in that the Government has not provided the Court with any insight into the overall nature of the TECS list, the standards, if any, that were used to determine an individual's placement on this list, or the significance, if any, of being designated as one for whom officials should 'lookout'").

179. *Cotterman*, 709 F.3d at 962–63.

cell phones and laptops make a forensic digital search especially intrusive—and analytically distinct from searches of other forms of property.[180] A forensic search provides law enforcement with access to a traveler's information in ways that are quantitatively and qualitatively different from routine border searches of physical belongings.[181] Modern electronic devices are capable of storing "warehouses full of information"—far more information about an individual than a person could physically travel with.[182] Moreover, electronic devices are not simply repositories for files that individuals routinely carry. Rather, they are "simultaneously offices and personal diaries" that "contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails."[183]

In a rejection of the logic of its earlier decision in *Arnold*, the Ninth Circuit concluded that the characteristics of a forensic digital search implicate important privacy and dignity interests protected by the Fourth Amendment because of the "uniquely sensitive nature of data on electronic devices."[184] The possibility of intruding upon these privacy and dignity interests is what distinguishes a forensic digital search from other kinds of property searches at the border such as disassembling a gas tank, as in *Flores-Montano*,[185] or drilling a hole in the bed of a pickup truck[186]—searches that have "little implication for an individual's dignity and privacy interests."[187] The court repudiated *Arnold*'s categorical approach to property searches, finding instead that what is reasonable under the Fourth Amendment "must account for differences in property."[188] That analysis must recognize that individuals and society have different expectations of privacy with respect to different kinds of property. While travelers expect searches of physical property at the border, they do not expect border agents to "mine every last piece of

180. *Id.* at 965 ("The point is technology matters.").

181. *Id.*

182. *Id.* at 964.

183. *Id.*

184. *Id.* at 966 (finding that a forensic digital search is "essentially a computer strip search. An exhaustive forensic search of a copied laptop hard drive intrudes upon privacy and dignity interests to a far greater degree than a cursory search at the border"); *cf. supra* notes 166–76 and accompanying text (describing the reasoning in *Arnold*).

185. *See* United States v. Flores-Montano, 541 U.S. 149, 150–51 (2004).

186. *See* United States v. Chaudhry, 424 F.3d 1051, 1054 (9th Cir. 2005).

187. *Cotterman*, 709 F.3d at 966 ("[T]he uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy and thus renders an exhaustive exploratory search more intrusive than with other forms of property.").

188. *Id.*

data on their devices or deprive them of their most personal property for days" absent some particularized suspicion.[189]

The court recognized the government's substantial interest in protecting the country from contraband, an interest that "may be heightened" by national crises such as drug smuggling or international terrorism.[190] But the court emphasized that "reasonableness remains the touchstone" of the Fourth Amendment, even at the border, and cautioned that the Supreme Court "has never endorsed the proposition that the goal of deterring illegal contraband at the border suffices to justify any manner of intrusive search."[191]

The majority defended the reasonable suspicion requirement as a "modest, workable standard" that law enforcement officials already apply in other contexts.[192] Responding to the dissent,[193] the majority reasoned that the practical considerations of border control—in particular, the "sheer number of international travelers"—are such that, "as a matter of commonsense and resources, it is only when reasonable suspicion is aroused that such searches typically take place."[194] The court concluded that the substantial privacy and dignity interests people have in digital information outweigh the government's interests in conducting a forensic digital border search without any suspicion.[195]

The *Cotterman* majority distinguished a forensic search from other digital border searches that it considered routine but failed to elaborate on the distinction.[196] For example, whereas the First Circuit created a list of factors for determining whether a particular search at the border was routine or nonroutine, the Ninth Circuit created no such framework for defining a forensic digital search in contrast to a manual one.[197] Instead, the Ninth Circuit largely left the details to law enforcement to "make a

189. *Id.* at 967–68 (internal citation omitted).

190. *Id.* at 966 (internal quotations omitted).

191. *Id.* at 967.

192. *Id.* at 966.

193. *See id.* at 985 (Smith, J., dissenting).

194. *Id.* at 967 n.14 (majority opinion).

195. *Id.* at 967–68.

196. Lower courts have had difficulty applying the distinction. *See* United States v. Kim, No. 13-cr-00100-ABJ, 2015 BL 134375, at *19–21 (D.D.C. May 8, 2015), *available at* https://cdn.arstechnica.net/wp-content/uploads/2015/05/kimruling.pdf; United States v. Saboonchi, 990 F. Supp. 2d 536, 552–58 (D. Md. 2014) ("[I]t is difficult to figure out the precise basis on which the Ninth Circuit distinguished forensic searches from conventional ones.").

197. *Compare Cotterman*, 709 F.3d at 967, *with* United States v. Braks, 842 F.2d 509, 511–12 (1st Cir. 1988) (listing factors for determining whether a particular body search at the border is routine or nonroutine).

commonsense differentiation between a manual review of files on an electronic device and application of computer software to analyze a hard drive."[198]

The court did state that the search in *Arnold* was permissible without reasonable suspicion, even while narrowing *Arnold* to its facts.[199] The court characterized the search in *Arnold* as a "quick look and unintrusive search."[200] Although the search in *Arnold* began as a brief look into two desktop folders, it ultimately lasted several hours.[201] As the *Saboonchi* court noted, the complete search in *Arnold* "hardly is 'quick' in the conventional sense and, to the contrary, actually shows how lengthy and comprehensive a conventional search can be."[202] The *Cotterman* majority's abbreviated discussion of the differences between forensic and manual digital searches and its approval of the digital search in *Arnold* illustrate the challenges of drawing a clear line between digital searches that are so intrusive as to require reasonable suspicion—or some higher standard—and those that do not.

2. United States v. Saboonchi

In *United States v. Saboonchi*, border agents confiscated and forensically searched two smartphones and a flash drive after stopping Ali Saboonchi and his wife, who were returning to New York after a day trip to Canada.[203] The government argued that the searches were routine

198. *Cotterman*, 709 F.3d at 967.

199. *Id.* at 960, 960 n.6.

200. *Id.* at 960.

201. United States v. Arnold, 533 F.3d 1003, 1005 (9th Cir. 2008). The district court found that the border agents had not established reasonable suspicion before conducting the search. *Id.*

202. United States v. Saboonchi, 990 F. Supp. 2d 536, 555 (D. Md. 2014). *Saboonchi* read *Cotterman*'s interpretation of *Arnold* broadly, to include the full search that took place. But there is a narrower reading as well. In *Cotterman*, the Ninth Circuit may have meant to include only the initial search of Arnold, which turned up the first photo, within its definition of a "quick . . . and unintrusive" digital search, given the fact that the initial search aroused enough suspicion that the border agents decided to dig further. For example, later in the opinion the majority emphasized that "suspicionless searches of the type approved in *Arnold* will continue; border officials will conduct further, forensic examinations where their suspicions are aroused by what they find or by other factors." *Cotterman*, 709 F.3d at 967. The court also contrasted a forensic search with a "cursory" search of a computer at the border. *Id.* at 966. In any case, the Ninth Circuit was not particularly clear on whether there are any limits for a nonforensic digital search at the border.

203. *Saboonchi*, 990 F. Supp. 2d at 539. The agents stopped Saboonchi and his wife for secondary questioning after Saboonchi turned up a hit on the Treasury Enforcement Communication System (TECS). *Id.* at 541. DHS had flagged Saboonchi, who is a dual citizen of the United States and Iran, in connection with suspicion that he may be violating restrictions on export to Iran. *Id.* at 539. The agents questioned Saboonchi and his wife separately and seized two smartphones and a flash drive. *Id.* The couple was then allowed to reenter the United States. *Id.* A DHS special agent

and therefore subject to no reasonable suspicion requirement under *Ickes*.[204] The court agreed that, under *Ickes*, "the mere fact that a search includes computer files does not transform it from routine to nonroutine."[205] Nevertheless, the court distinguished *Ickes* on the grounds that it did not address forensic digital searches.[206] It concluded that such searches are "sui generis" and require reasonable suspicion.[207]

The court reached the same result as the Ninth Circuit in *Cotterman* but went much further in its analysis as to why forensic searches are uniquely intrusive. The court identified three factors that differentiate forensic digital searches from other digital searches.[208] First, because a forensic search requires making an exact copy of the electronic device's hard drive, it does not present the same time constraints and allows border agents to complete the search long after the individual has left the border.[209] A forensic search allows for an exhaustive search of all information on the device in a way that a manual search of a computer in the border context would be unable to replicate.[210] Even a lengthy seizure may raise questions if it is not "reasonably related in scope to the circumstances which justified it initially."[211]

Second, the use of specialized software in a forensic search provides access to previously deleted information and unsaved data.[212] This limits the traveler's ability to choose what to travel with.[213] In a world of suspicionless forensic digital searches, a traveler who wishes to maintain private or confidential records "would be well advised *never* to put private or personal data on her computer or smartphone."[214] It is this

---

subsequently conducted a forensic search of the smartphones and flash drive. *Id.* at 539–40.

204. *Id.* at 544, 546.

205. *Id.* at 546; *see also id.* at 554 ("At the very least, *Ickes* forecloses the possibility that the mere fact that an electronic device may contain massive amounts of personal data, by itself, can change the legal analysis at the border . . . .").

206. *Id.* at 546.

207. *Id.* at 568.

208. *Id.* at 564.

209. *Id.* at 564–66.

210. *Id.*; *see also id.* at 547 ("No matter how thorough or highly motivated the agent is, a manual search of a computer or digital device will never result in the human visualization of more than a fraction of the content of the device.").

211. *Id.* at 565 (quoting United States v. Montoya de Hernandez, 473 U.S. 531, 543 (1985)) (internal quotation marks omitted).

212. *Id.* at 566–67.

213. *Id.* at 567; *cf.* Abidor v. Napolitano, 990 F. Supp. 2d 260, 277 (E.D.N.Y. 2013) (arguing that travelers should "[t]hink twice about the information [they] carry on [their] laptop" (first alteration in original)).

214. *Saboonchi*, 990 F. Supp. 2d at 567 (emphasis in original).

aspect of forensic digital searches that "stretches the computer-to-closed-container analogy beyond its breaking point."[215] Third, a forensic search provides access to location information and other metadata that can reveal intimate information about a person, including even domestic activities traditionally protected by the Fourth Amendment.[216] These factors led the court to conclude that "[i]t is difficult to conceive of a property search more invasive or intrusive than a forensic computer search—it essentially is a body cavity search of a computer."[217]

Despite strong language about the privacy and dignity interests in digital information, and acknowledgement that manual digital border searches could be "deeply probing" and "invasive,"[218] the court maintained that manual digital border searches do not require any level of suspicion.[219] The court reasoned that a manual digital border search is limited by the practicalities of the border context—especially the amount of time border agents can spend searching computers and cell phones.[220] The court was constrained by *Ickes*, which may have compelled that conclusion.[221] The problem is that, while the court rejected the container analogy for forensic digital searches, it oddly reaffirmed it for other digital searches.[222] In the court's view, a digital border search can be analogized to the search of a suitcase, even if a forensic search cannot:

> [A manual digital] search has the same inherent limitations—and the same inherent risk of invasiveness—irrespective of what is being searched. There is only a finite amount of time available for a CBP agent to detain a traveler at the border to search the contents of his suitcase or laptop.[223]

Although *Saboonchi* and *Cotterman* have important differences,[224]

---

215. *Id.*

216. *Id.* at 568–69 ("[A] Customs officer performing a forensic search can recreate the most intimate details of a person's life over the course of the last several months—even if the data includes highly personal details of what transpired before leaving the country or while in one's own home.").

217. *Id.* at 569.

218. *Id.* at 547.

219. *Id.* at 569. The court used the term "conventional" computer search to describe any digital search that is nonforensic, i.e., manual digital searches. *See supra* notes 141–53 and accompanying text.

220. *Id.* at 564.

221. *Id.* at 569.

222. *Id.* at 564.

223. *Id.*

224. In particular, *Saboonchi* provides a more robust distinction between forensic digital searches and other digital searches. *Cf. supra* notes 196–202, 208–17 and accompanying text.

their broad strokes are similar. Both decisions establish that forensic digital searches are nonroutine and must be supported by reasonable suspicion.[225] Both also reject analogies between forensic digital searches and searches of physical property, such as items in closed containers.[226] And yet, perhaps both courts did not embrace their own analyses enough. Both allow manual digital searches without suspicion.[227] In this regard, both decisions allow digital fishing expeditions at the border, so long as they are carried out manually—which cuts against the Fourth Amendment requirement that searches be limited in scope.[228] On all of these points, prior case law played a role. *Arnold* and *Ickes* shaped *Cotterman* and *Saboonchi* in significant ways, perhaps preventing the courts in both cases from considering the full range of standards available under the Fourth Amendment.

III. DIGITAL BORDER SEARCHES 3.0: HOW SHOULD COURTS REGULATE DIGITAL BORDER SEARCHES AFTER *RILEY v. CALIFORNIA*?

The Supreme Court has not yet decided what level of process the Fourth Amendment requires for a digital border search.[229] But its decision in *Riley v. California* provides relevant guidance. Whereas the courts in *Cotterman* and *Saboonchi* were constrained by precedent,[230]

---

225. United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013); *Saboonchi*, 990 F. Supp. 2d at 539.

226. *Cotterman*, 709 F.3d at 964; *Saboonchi*, 990 F. Supp. 2d at 567.

227. *Cotterman*, 709 F.3d at 959; *Saboonchi*, 990 F. Supp. 2d at 547. In *Abidor v. Napolitano*, the court declined to hold that reasonable suspicion is required for a forensic digital search because it would have no practical effect on current practice and may have a "chilling effect" on border officials. 990 F. Supp. 2d 260, 282 (E.D.N.Y. 2013). Nevertheless, the court "agree[d] with the Ninth Circuit that, if suspicionless forensic computer searches at the border threaten to become the norm, then some threshold showing of reasonable suspicion should be required." *Id.*

228. *See* New Jersey v. T.L.O., 469 U.S. 325, 341 (1985) (requiring courts to "determine whether the search as actually conducted 'was reasonably related in scope to the circumstances which justified the interference in the first place'" (citation omitted)).

229. United States v. Kim, No. 13-cr-00100-ABJ, 2015 BL 134375, at *10 (D.D.C. May 8, 2015), *available at* https://cdn.arstechnica.net/wp-content/uploads/2015/05/kimruling.pdf.

230. The Ninth Circuit's distinction between forensic digital border searches and other digital border searches was central to its rationale in *Cotterman* and allowed it to affirm *Arnold* while narrowing that decision to its facts. *See Cotterman*, 709 F.3d at 967 (distinguishing between forensic and other digital searches); *id.* at 960 n.6 (narrowing *Arnold*). In *Saboonchi*, the court emphasized its opinion was consistent with the Fourth Circuit's decision in *Ickes*. *See Saboonchi*, 990 F. Supp. 2d at 552 ("*Ickes* makes it clear that a routine border search may include a conventional inspection of electronic media and a review of the files on them just as it may include physical papers."); *id.* at 560 ("[T]he Fourth Circuit has stated [in *Ickes*] that a conventional search of a computer is not legally distinct from a conventional search of a closed container.").

resulting in a limited debate over whether forensic digital searches require reasonable suspicion, *Riley* opens up a doctrinal path to reexamine digital border searches. In doing so, courts should consider the full range of standards provided by Fourth Amendment doctrine: a warrant based on probable cause, probable cause without a warrant, reasonable suspicion, or no suspicion at all. Indeed, courts and litigants have already begun debating *Riley*'s impact on this issue. Two federal district courts have interpreted *Riley*'s applicability to digital border searches in different ways.[231] The defendant in one of those cases has argued on appeal to the Fourth Circuit that *Riley* changes the digital border search analysis.[232] This Part discusses *Riley*, its implications for digital border searches, how two lower courts have analyzed digital border searches after the decision, and considerations for courts moving forward.

A. Riley *and the New Digital Search Calculus*

The Supreme Court held in *Riley* that police must obtain a warrant before searching the digital information on a cell phone incident to an individual's arrest.[233] The Court recognized that a search of digital information in a cell phone is categorically different from a search of one's person or physical effects.[234] To determine whether to exempt searches of cell phones incident to arrest from the warrant requirement, the Court applied a balancing test weighing the state's interests in security and retaining evidence against the individual's privacy interests.[235] The Court concluded that digital information carries substantial privacy interests and is qualitatively and quantitatively different from any physical items individuals typically carry.[236] The

231. *See* United States v. Saboonchi, No. 13-cr-00100, 2014 BL 207375, at *1 (D. Md. July 28, 2014), *available at* https://cdn.arstechnica.net/wp-content/uploads/2015/05/kimruling.pdf (rejecting motion for reconsideration in light of *Riley*, concluding that *Riley* does not change the border search exception and that the court's decision is consistent with *Riley* anyway); *Kim*, 2015 BL 134375, at *20–22 (concluding that *Riley* gives courts clear guidance on digital border search analysis); Brief of Appellant, *supra* note 27, at 8–9 (arguing that under *Riley* digital border searches must be subjected to the warrant requirement); *see also* LAFAVE, *supra* note 64, § 10.5(f), at 7–8 (noting that "*Cotterman* certainly is bolstered" by *Riley* but that it is an open question "whether post-*Riley* courts will conclude that *Cotterman* does not go far enough").

232. *See* Brief of Appellant, *supra* note 27, at 8–9; Brief of Amicus Curiae ACLU, *supra* note 27, at 2–3; Brief of Amicus Curiae EFF, *supra* note 27, at 3.

233. Riley v. California, __ U.S. __, 134 S. Ct. 2473, 2495 (2014).

234. *Id.* at 2489–91.

235. *Id.* at 2484–85.

236. *Id.* at 2489–91.

Court also found that the government's interests in officer safety and preventing the destruction of evidence with regard to digital information are not significant enough to justify a departure from the warrant requirement.[237]

The Court put technology at the center of its analysis, deciding the question of "how the search incident to arrest doctrine applies to modern cell phones."[238] The decision involved two cases and two types of cell phones: *Riley v. California* (smartphone)[239] and *United States v. Wurie*[240] (flip phone).[241] The Court has recognized that searches incident to arrest—where officers search an arrestee's person or property found on or within the immediate control of the arrestee—are reasonable even without a warrant to: (1) protect officer safety and effectively carry out the arrest or (2) prevent the destruction of evidence.[242] In resolving the issue, the Court rejected a "mechanical application" of its precedents in favor of reexamining the doctrine's applicability in light of the fact that smartphones and flip phones "are based on technology nearly inconceivable just a few decades ago," when the Court decided its leading search incident to arrest cases.[243]

---

237. *Id.* at 2485–87.

238. *Id.* at 2484.

239. In *Riley*, police searched the smartphone of David Riley after stopping him for driving with expired registration tags. The officer discovered that Riley's license was suspended and impounded the car, while another officer conducted an inventory search of the car, finding two handguns hidden under the car's hood. The officers then arrested Riley for possession of concealed and loaded firearms. One officer also searched Riley's person, discovering a smartphone in his pocket. The officer began searching the cell phone. The officer noticed some words preceded by the letters "CK," a label he believed stood for "Crip Killers," a slang term for members of the Bloods gang. A detective at the police station further examined the contents of the phone, looking for evidence, and found photographs of Riley standing in front of a car they suspected had been involved in a shooting a few weeks earlier. Riley was ultimately charged in connection with the earlier shooting. *Id.* at 2480–81.

240. 612 F. Supp. 2d 104 (D. Mass. 2009), *rev'd*, 728 F.3d 1 (1st Cir. 2013), *aff'd sub nom. Riley*, 134 S. Ct. 2473.

241. In *Wurie*, police officers seized a "flip phone," a cell phone with more-limited features than a smartphone, after arresting Brima Wurie on suspicion of making a drug sale. The phone received several incoming calls from a number labeled "my house" shortly after the officers took Wurie to the police station. The officers opened the phone, saw a picture of a woman and a baby set as the wallpaper, accessed the call log, and viewed the number named "my house." The officers traced the phone to an apartment building, saw a woman that appeared to be the one on the phone's wallpaper, and then obtained a warrant to search the apartment. *Riley*, 134 S. Ct. at 2481.

242. *Id.* at 2483–84; Arizona v. Gant, 556 U.S. 332, 338–40 (2009); United States v. Robinson, 414 U.S. 218, 230–34 (1973); Chimel v. California, 395 U.S. 752, 762–63 (1969). "If there is no possibility that an arrestee could reach into the area that law enforcement officers seek to search, both justifications for the search-incident-to-arrest exception are absent and the rule does not apply." *Arizona*, 556 U.S. at 339.

243. *Riley*, 134 S. Ct. at 2484.

Under a balancing test used to determine whether to depart from the warrant requirement, the Court assessed "the degree to which [the type of search] intrudes upon an individual's privacy" against "the degree to which it is needed for the promotion of legitimate governmental interests."[244] In conducing this analysis, the Court asked whether applying the search incident to arrest doctrine to cell phones would "untether the rule from the justifications underlying the . . . exception."[245]

The Court first identified the government's interests under *Chimel v. California*[246] in security and preventing the destruction of evidence.[247] To protect these interests, the Court concluded that officers may still conduct a physical search of the cell phone.[248] But because digital data itself cannot be used to physically harm an arresting officer, the government has little interest in immediately searching it on the basis of officer safety.[249] Similarly, once the officer has the phone in custody, the arrestee cannot erase any evidence accessible through the phone. The Court did consider the government's argument that digital evidence could be destroyed by remote wiping by absent third parties, but found that too distant from the government's interests under *Chimel*, which are directly tied to the arrestee's attempt to destroy or hide evidence at the scene of arrest.[250] More important, the government can simply prevent remote wiping by disconnecting the phone from the network.[251] Thus, while the government generally has substantial interests in security and preservation of evidence at the scene of an arrest, those interests are significantly lessened with respect to digital information in the search incident to arrest context.[252]

The Court then assessed the individual interests in protecting digital information. In particular, *Riley* establishes that the "immense storage

244. *Id.* at 2484–85.

245. *Id.* at 2485.

246. 395 U.S. 752 (1969).

247. *Riley*, 134 S. Ct. at 2483.

248. "[O]fficers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon." *Id.* at 2485; *cf. supra* notes 141–42 and accompanying text (discussing a "physical device search").

249. *Riley*, 134 S. Ct. at 2485.

250. *Id.* at 2485–86. "Remote wiping occurs when a phone, connected to a wireless network, receives a signal that erases stored data. This can happen when a third party sends a remote signal or when a phone is preprogrammed to delete data upon entering or leaving certain geographic areas (so-called 'geofencing')." *Id.* at 2486.

251. *Id.* at 2487.

252. *Id.* at 2485.

capacity" of modern cell phones marks a quantitative difference from other physical items people typically carry.[253] The storage capacity of modern cell phones has several "interrelated consequences for privacy."[254] First, it collects in one place many different kinds of information—photos, picture messages, text messages, internet browsing history, a calendar, a thousand-entry phone book, etc.—that reveal more information than any isolated record.[255] Second, digital information accessible via cell phones allows a search to reveal information that is not even stored on the phone.[256] Third, data on or accessible through the phone can date back to the purchase or even earlier.[257] Fourth, there is an element of "pervasiveness that characterizes cell phones but not physical records."[258] Almost everyone carries around "a digital record of nearly every aspect of their lives—from the mundane to the intimate."[259]

Cell phones also present qualitative differences.[260] Internet searches and browsing history can reveal an individual's private interests or concerns, and the location information retained by cell phones can reveal where an individual has been.[261] Cell phone apps manage detailed information about one's life, from political affiliation to addictions, prayer, tracking pregnancy and other health symptoms, planning one's budget, and improving one's love life.[262]

The unique quantitative and qualitative aspects of digital information stored on or accessed by a cell phone persuaded the Court to conclude that searching a phone is even more intrusive than searching a home:

> Indeed, a cell phone search would typically expose to the

253. *Id.* at 2489 (noting that a typical smartphone has a storage capacity of sixteen gigabytes, which translates to millions of pages of text, thousands of pictures, or hundreds of videos).

254. *Id.*

255. *Id.*

256. *Id.* ("The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet.").

257. *Id.* ("A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.").

258. *Id.* at 2490.

259. *Id.*; *see also* Scott Skinner-Thompson, *Outing Privacy*, 110 NW. U. L. REV. 159, 208–09, 214 (2015) (discussing *Riley*'s emphasis on the heightened importance of intimate and political information, both accessible via searches of cell phones).

260. *Riley*, 134 S. Ct. at 2490.

261. *Id.* ("Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.").

262. *Id.*

> government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.[263]

Weighing the intrusiveness of a digital search against the government's interests in officer safety and preservation of evidence, the Court held that officers must generally secure a warrant before searching a cell phone incident to arrest.[264]

B. The Implications of Riley*: Digital Is Different*

Riley clarifies an important doctrinal debate over digital searches. Prior to *Riley*, lower courts were split over two different approaches.[265] Courts debated whether digital information is merely physical evidence in digital form, such that traditional rules of search and seizure apply, or something qualitatively different, requiring new analysis under the Fourth Amendment.[266]

Under one theory, courts should treat digital files like paper documents and computers like filing cabinets or containers—mere repositories for digital documents.[267] Thus the government does not need to specify whether it is searching for digital or paper documents, and courts look to traditional methods of limiting searches to ensure they are conducted reasonably—for example, by limiting a search according to the nature of the criminal activity alleged or the nature of the evidence sought.[268] Perhaps the most significant consequence of this theory is that officers may broadly search digital information in order to ascertain what it is[269] and may seize any evidence in "plain view" pursuant to a

263. *Id.* at 2491.

264. *Id.* at 2484–85.

265. *See* CLANCY, *supra* note 47, § 12.4.8.2, at 684–98.

266. *Id.* § 12.4.8.2, at 684–85.

267. *Id.* § 12.4.8.2.1, at 686 n.166 (collecting cases); *see also* U.S. DEP'T OF HOMELAND SEC., *supra* note 42, at 7.

268. *See* CLANCY, *supra* note 47, § 12.4.8.2.1, at 686–89.

269. This supposedly follows from *Andresen v. Maryland*, 427 U.S. 463 (1976), in which the Court accepted cursory examination of documents in order to verify which ones were within the proper scope of the search:

> In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized . . . . [R]esponsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.

Id. at 482 n.11.

justified intrusion.[270] As one court explained:

> [Police officers] may search the location authorized by the warrant, including any containers at that location that are reasonably likely to contain items described in the warrant. . . . This container rationale is equally applicable to nontraditional, technological "containers" that are reasonably likely to hold information in less tangible forms.[271]

Analogizing computers to containers rests on the assumption that the technological differences between them amount to little, so far as Fourth Amendment doctrine is concerned.

Other courts have instead adopted a "special approach."[272] Under this theory, the container/filing cabinet analogy fails to account for the technological differences between digital information and physical objects.[273] Computers offer a fundamentally different system of storage and information, present unique privacy concerns—particularly in light of the plain view doctrine—and provide ways in which to minimize the intrusiveness of a digital search.[274] At least one author of a Fourth Amendment treatise argued ahead of *Riley* that the special approach has "no foundation in Fourth Amendment jurisprudence, even by

---

270. CLANCY, *supra* note 47, § 12.4.8.2, at 684. Under the plain view doctrine, an officer may size evidence without a warrant if (1) the officer is in a legitimate position to see the evidence, (2) the officer is in a location to seize the evidence lawfully, and (3) the incriminating character of the evidence is immediately apparent. *See* Horton v. California, 496 U.S. 128, 136–37 (1990); CLANCY, *supra* note 47, § 7.4.2.4, at 378. The Court has stated the rationale for the plain view doctrine is:

> [I]f contraband is left in open view and is observed by a police officer from a lawful vantage point, there has been no invasion of a legitimate expectation of privacy and thus no 'search' within the meaning of the Fourth Amendment—or at least no search independent of the initial intrusion that gave the officers their vantage point.

Minnesota v. Dickerson, 508 U.S. 366, 375 (1993). But the plain view doctrine cannot be used to turn a somewhat limited intrusion into a general search. As Justice Stewart stated for the plurality in *Coolidge v. New Hampshire*, 403 U.S. 443 (1971), "the 'plain view' doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges." *Id.* at 466.

271. People v. Gall, 30 P.3d 145, 153 (Colo. 2001) (en banc); *see also* United States v. Arnold, 533 F.3d 1003, 1007 (9th Cir. 2008) ("Courts have long held that searches of closed containers and their contents can be conducted at the border without particularized suspicion under the Fourth Amendment.").

272. CLANCY, *supra* note 47, § 12.4.8.2.2, at 689–98; *see, e.g.*, United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010) (en banc); United States v. Payton, 573 F.3d 859 (9th Cir. 2009); United States v. Burgess, 576 F.3d 1078 (10th Cir. 2009); United States v. Carey, 172 F.3d 1268 (10th Cir. 1999); *see also* Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75 (1994).

273. *See* United States v. Saboonchi, 990 F. Supp. 2d 536, 567 (D. Md. 2014).

274. *See* CLANCY, *supra* note 47, § 12.4.8.2.3, at 692–94.

analogy,"[275] and that the Court's prior refusal to rank different types of containers by privacy interest[276] would lead the Court to reject the special approach for "electronic device containers."[277]

The doctrinal debate over how to treat digital information under the Fourth Amendment formed a major part of the backdrop to *Riley* and explains at least part of that decision's significance.[278] In rejecting the federal government's argument that a search of data on a cell phone is "materially indistinguishable" from searches of physical items, the Court said:

> That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.[279]

The Court's categorical language—"cell phones, as a category"—demonstrates the Court's emphatic rejection of the view that the digital information stored on cell phones and computers may always be searched according to the same rules as physical items.[280] The Court

---

275. *Id.* § 12.4.8.2.3, at 692.

276. The Court rejected the proposition that there was any Fourth Amendment distinction between "worthy" and "unworthy" containers:

> For just as the most frail cottage in the kingdom is absolutely entitled to the same guarantees of privacy as the most majestic mansion, so also may a traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf claim an equal right to conceal his possessions from official inspection as the sophisticated executive with the locked attaché case.

United States v. Ross, 456 U.S. 798, 822 (1982).

277. CLANCY, *supra* note 47, § 12.4.8.2.3, at 697.

278. One scholar wrote in reaction to the decision that *Riley* would usher in more doctrinal change:

> In a nearly unanimous opinion packed with references to gigabytes, apps, and the cloud, Chief Justice John Roberts proved that the Justices get it. They get that digital technologies are different from anything our culture has seen before. They get that people are using those technologies in a million dynamic ways that were unimaginable a generation ago. And they get that, in at least some contexts, the Old Rules need to change.

Richard M. Re, *Symposium: Inaugurating the Digital Fourth Amendment*, SCOTUSBLOG (June 26, 2014, 12:37 PM), http://www.scotusblog.com/2014/06/symposium-inaugurating-the-digital-fourth-amendment/.

279. Riley v. California, __ U.S. __, 134 S. Ct. 2473, 2488–89 (2014).

280. *Id.* at 2489 ("Cell phones differ in both a quantitative and a qualitative sense from other

further noted that advances in cloud computing—which allow users of cell phones and other networked devices to access data stored remotely[281]—underscore the differences between modern cell phones and physical containers. "Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter. But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen."[282]

C. Riley*'s Relevance to Border Searches*

Two federal courts have considered the effect of *Riley* on digital border searches.[283] They have disagreed over whether the analysis in *Riley* applies and, even if it does apply, the extent to which it changes how courts must regulate digital border searches.

1. United States v. Saboonchi

Saboonchi filed a motion for reconsideration after *Riley*, arguing that the Supreme Court decision changes the digital border search analysis.[284] The court denied the motion on two grounds: (1) that *Riley* "did not touch on the border search exception" and (2) the court's previous decision was consistent with the principles outlined in *Riley*.[285] On the first point, the court in *Saboonchi* reasoned that *Riley* "did not recognize a categorical privilege for electronic data," and expressly noted that other exceptions, such as in exigent circumstances, may still justify the warrantless search of a cell phone.[286] In the court's view, this indicated that the Supreme Court did not intend to "exempt cell phones from all

---

objects that might be kept on an arrestee's person. The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."). "Cloud computing is the capacity of internet-connected devices to display data stored on remote servers rather than on the device itself." *Id.* at 2491.

281. *See* Lon A. Berk, *After* Jones*, the Deluge: The Fourth Amendment's Treatment of Information, Big Data and the Cloud*, 14 J. HIGH TECH. L. 1, 4–6 (2014) (explaining how cloud computing allows users of cell phones and other networked devices to access data stored on remote servers).

282. *Riley*, 134 S. Ct. at 2491 (citation omitted).

283. United States v. Saboonchi, 48 F. Supp. 3d 815, 816 (D. Md. 2014); United States v. Kim, No. 13-cr-00100-ABJ, 2015 BL 134375 (D.D.C. May 8, 2015), *available at* https://cdn.arstechnica.net/wp-content/uploads/2015/05/kimruling.pdf.

284. *Saboonchi*, 48 F. Supp. 3d at 816.

285. *Id.*

286. *Id.* at 817.

warrantless searches."[287] The court also reasoned that the Supreme Court has limited searches incident to arrest with respect to closed containers, whereas it has always indicated that suspicionless searches of containers are permitted under the border search exception.[288]

On the second point, the court concluded that *Riley* supports the conclusion that forensic digital searches are qualitatively different from other digital searches.[289] The court acknowledged that the search in *Riley* was not forensic, but explained that "the underlying logic in the two cases is the same."[290] The invasiveness of the search "is only part of the puzzle."[291] Moreover, the court reasoned, *Riley* did not change the government's interests in national security and immigration and customs enforcement in the border context.[292] Applying the balancing test, the court agreed that cell phones deserve the "highest level of Fourth Amendment protection available," but could not find "a single case" requiring anything more than reasonable suspicion in the border context.[293]

2. United States v. Kim

The District Court for the District of Columbia took a different approach in *United States v. Kim*.[294] The court embraced *Riley* as a decision giving courts clear guidance that is directly applicable to digital border searches.[295] The court ruled in favor of Kim's motion to suppress evidence extracted from his laptop, which federal agents had seized from him when he was leaving the country at the Los Angeles International Airport.[296]

DHS investigators suspected Kim, who had business operations in California and Korea, was involved in a 2008 shipment of aircraft parts used in aircraft and missile systems to a Chinese businessman in Korea, who then sent them on to customers in Iran, in violation of the federal

287. *Id.* at 818.

288. *Id.*

289. *Id.* at 819.

290. *Id.*

291. *Id.*

292. *Id.*

293. *Id.*

294. No. 13-cr-00100-ABJ, 2015 BL 134375 (D.D.C. May 8, 2015), *available at* https://cdn.arstechnica.net/wp-content/uploads/2015/05/kimruling.pdf.

295. *Id.* at *20–21.

296. *Id.* at *1, *26.

trade embargo.[297] The special agent in charge of the investigation decided to stop Kim the next time he left the country to search his laptop for evidence in support of the allegation.[298] The agent stopped Kim just before Kim boarded his flight and took his laptop, informing him that he was conducting a border search and would return the computer once the search was complete.[299] The agent permitted Kim to board his flight.[300]

The agent did not search the laptop at the airport. Instead, he sent it to DHS's San Diego Computer Forensics Group and "requested a border search of the laptop."[301] The agent in charge of the computer search created a forensic image, or duplicate copy, of Kim's hard drive, so that the agent could read and analyze "every single piece of data on the hard drive."[302] The agent used specialized software to extract, process, and identify thousands of files matching keywords suggested by the first agent.[303] The first agent spent "several days" reviewing the files, which supported the allegations against Kim, leading to criminal charges.[304] After the search, the first agent applied for a search warrant to conduct "forensic imaging . . . and identification and extraction of relevant data"[305]—even though, as the court noted, that search had already been completed.[306]

Federal prosecutors made three arguments for why the search was permissible. First, they argued that the search was allowed under *Ramsey* because "a laptop is nothing more than a sort of container."[307] This argument is somewhat remarkable, given the Supreme Court's clear rejection of analogizing cell phones to containers in *Riley*.[308] The court dismissed this line of reasoning on that basis.[309] The government also

297. *Id.* at *1–2.

298. *Id.* at *1; *see also id.* at *25 ("[T]he investigators' sworn testimony to the Court made it clear that the primary, if not the sole, purpose of the pre-planned encounter at the border was to obtain the laptop and search it for evidence.").

299. *Id.* at *6–7.

300. *Id.* at *7.

301. *Id.*

302. *Id.*

303. *Id.* at *7–8.

304. *Id.* at *13.

305. *Id.* at *9.

306. *Id.* at *1–2, *26. Both special agents testified that no search occurred after the warrant was approved. *Id.* at 26.

307. *Id.* at *10.

308. *See* Riley v. California, __ U.S. __, 134 S. Ct. 2473, 2488–89, 2491 (2014); *supra* Part III.B.

309. *Kim*, 2015 BL 134375, at *23 ("*Riley* indicates that the Fourth Amendment is not necessarily satisfied by a simplistic likening of a computer to a searchable 'container.'"); *see also*

argued that the search was lawful either as a routine border search or, alternatively, as a forensic search supported by reasonable suspicion.[310]

The court first addressed whether the government established reasonable suspicion, and found that it did not.[311] In particular, the court concluded that the basis for the search was the agent's expectation that the computer contained evidence of *past* criminal activity, "but there was no objective manifestation that Kim was or was 'about to be engaged' in criminal activity at the time."[312] With respect to Kim's travel, "the search was nothing more than a fishing expedition"—a factor that distinguished the search in *Kim* from those in *Cotterman* and the recent decision in *United States v. Hassanshahi*.[313]

The court then examined whether the search was "forensic," as in *Cotterman* and *Saboonchi*, or routine. It found that the search "fell somewhere on the spectrum between the two poles described by other courts."[314] The agents did not search through deleted files, but they copied the entire hard drive and could have conducted a more comprehensive search if necessary.[315] The government argued the use of forensic software was not essential to the search because anyone with unlimited time could locate the same files.[316] Nevertheless, the agents confiscated the computer, created an exact copy of the hard drive, used whatever software they determined necessary for the search, and kept a copy of the data for "a period of unlimited duration."[317] "Certainly no one simply turned it on and perused the files as might have been possible at the border."[318]

The lack of a clear distinction between a forensic search requiring reasonable suspicion and a routine border search persuaded the court to turn to *Riley*'s balancing test.[319] Under *Riley*, analyzing the

---

id. at *17 ("[G]iven the vast storage capacity of even the most basic laptops, and the capacity of computers to retain metadata and even deleted material, one cannot treat an electronic storage device like a handbag simply because you can put things in it and then carry it onto a plane.").

310. *Id.* at *10.

311. *See id.* at *13.

312. *Id.*

313. 75 F. Supp. 3d 101 (D.D.C. 2014); *Kim*, 2015 BL 134375, at *13.

314. *Kim*, 2015 BL 134375, at *20.

315. *Id.* at *19.

316. *Id.* at *19–21.

317. *Id.* at *19.

318. *Id.*

319. *Id.* at *20. The government's "forensic specialist also acknowledged that the term 'forensic search' can describe a range of examinations and that the term has no specific definition." *Id.* at *19.

reasonableness of a digital search that begins at the border "does not simply end with the invocation of a statute or the well-recognized border exception, as broad as it may be, and it does not turn on the application of an undefined term like 'forensic.'"[320] As in *Riley*, the court considered whether applying the border search exception to digital searches at the border would "untether the rule from the justifications" underlying the exception.[321]

The court reasoned that travelers leaving the country implicated only the government's interest in exporting regulations, in contrast to government interests implicated by travelers entering the country, such as protecting national security and preventing smuggling.[322] The court concluded that, "while the immediate national security concerns were somewhat attenuated, the invasion of privacy was substantial."[323] Whatever the line between a forensic and a conventional digital search, "this search was qualitatively and quantitatively different from a routine border examination, and therefore, it was unreasonable given the paucity of grounds to suspect that criminal activity was in progress."[324]

The court questioned whether the digital search that took place "can accurately be characterized as a border search at all."[325] The court noted that the laptop may have been seized at the border, but it was then transported 150 miles away to a facility in San Diego, where DHS copied the hard drive and thoroughly searched the copy over a period of weeks. [326] DHS found nothing suspicious in Kim's luggage, permitted him to board his flight, and returned his laptop to him.[327] The actual search took place away from the border, involved a detailed list of keywords, and took weeks to complete, while the subject of the search was allowed to cross the border unhindered.[328] For these reasons, the search "did not possess the characteristics of a border search or other regular inspection procedures. It more resembled the common nonborder search based on individualized suspicion, which must be prefaced by the usual warrant and probable cause standards."[329]

---

320. *Id.* at *22.

321. *Id.*

322. *Id.* at *23–24.

323. *Id.* at *24.

324. *Id.*

325. *Id.*

326. *Id.*

327. *Id.*

328. *Id.*

329. *Id.* at *25 (quoting United States v. Brennan, 538 F.2d 711, 716 (5th Cir. 1976)) (internal

The government initially filed a notice of appeal but later moved to dismiss.[330]

D. How Riley *Changes the Digital Border Search Doctrine*

The Court has described the border search exception as similar to the search incident to arrest exception.[331] Both exceptions involve situations where the government has specific heightened interests and the subject of the search has a reduced expectation of privacy.[332] *Riley* suggests that courts should reconsider the developing digital border search doctrine. In particular, courts should consider afresh whether to extend the border search exception to searches of digital information in light of changes in technology and societal expectations.[333] Would applying the border search exception to a search of digital information that begins at the border "untether the rule from the justifications" underlying the exception?[334]

The border search doctrine has been traditionally associated with the federal government's right to prevent unwanted people and contraband from entering the country to protect national security, regulate immigration, and enforce customs restrictions.[335] The Court articulated the doctrine long before the development and widespread use of laptop computers, smartphones, and cloud computing. *Riley* recognized the gap between the search incident to arrest exception and these technological changes as grounds for reexamining the doctrine.[336] After *Riley*, the time is ripe for a reassessment to properly account for the differences between a search for digital information—which may not even be stored locally

---

quotation marks omitted).

330. Appellant United States of America's Unopposed Motion for Voluntary Dismissal of Interlocutory Appeal Pursuant to Rule 42(b), United States v. Kim, No. 15-03035 (D.C. Cir. Aug. 11, 2015).

331. United States v. Ramsey, 431 U.S. 606, 621 (1972) (describing the border search exception as "like the similar 'search incident to lawful arrest' exception").

332. *See* Riley v. California, __ U.S. __, 134 S. Ct. 2473, 2488 (2014) ("The search incident to arrest exception rests not only on the heightened government interests at stake in a volatile arrest situation, but also on an arrestee's reduced privacy interests upon being taken into police custody."); United States v. Montoya de Hernandez, 473 U.S. 531, 539–40 (1985) ("[N]ot only is the expectation of privacy less at the border than in the interior . . . the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is also struck much more favorably to the Government at the border." (citations omitted)).

333. *See Riley*, 134 S. Ct. at 2484.

334. *See id.* at 2485; *Kim*, 2015 BL 134375, at *22.

335. *See Ramsey*, 431 U.S. at 619; *supra* Part I.B.

336. *Riley*, 134 S. Ct. at 2484.

on the device[337]—and searches of a person, luggage, or vehicle.

Riley shows courts how to analyze this question. In deciding whether to exempt digital searches at the border from the baseline warrant requirement, courts must balance the intrusiveness of the search against the governmental interests that have traditionally justified the exception.[338] If courts find that the border exception does not apply to digital border searches, they must revert to the baseline warrant requirement.[339] But even if they find that the exception does apply, *Riley* weighs in favor of greater Fourth Amendment protection and a higher level of suspicion required for all digital border searches.

1. Individual Interests

Riley is particularly instructive with respect to the individual interests implicated by digital searches. The decision provides three main insights.

First, courts no longer have to guess as to the intrusiveness of a digital search; *Riley* recognizes there are significant privacy implications.[340] Indeed, the Court found that digital searches can be even more intrusive than the search of an individual's home—which has traditionally received the highest protection under the Fourth Amendment.[341] This finding alone would justify the conclusion that a digital search is beyond the scope of the traditional border search doctrine.

Second, *Riley* makes it clear that digital searches of smartphones and computers are categorically different from searches of luggage.[342] This conclusion finally discredits the analogy between computers and filing

---

337. Some may wonder whether the fact that data is stored in the cloud rather than locally on a device should result in less Fourth Amendment protection under the third-party doctrine. *But see* Ryan Watzel, *Riley's Implications for Fourth Amendment Protection in the Cloud*, 124 YALE L.J. F. 73, 73–74 (2014) (arguing that *Riley* suggests the Court's willingness to reconsider the third-party doctrine and recognize Fourth Amendment protection for personal data stored in the cloud); Shappert, *supra* note 24, at 13 (recommending that, after *Riley*, border officials disconnect electronic devices from networks and obtain a warrant before searching remotely stored data).

338. *Riley*, 134 S. Ct. at 2484–85.

339. *See id.* at 2482.

340. *See supra* notes 253–63, and accompanying text. It would be difficult for courts to argue that laptops and tablets deserve less protection than cell phones. In *Riley*, the Court compared cell phones to computers to illustrate the intrusiveness of searching them: "The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone." *Riley*, 134 S. Ct. at 2489.

341. *Riley*, 134 S. Ct. at 2491 (noting that phones contain sensitive records typically found in a home as well as private information that is not found in the home).

342. *See supra* Part III.B.

cabinets—on which *Arnold* and *Ickes* expressly relied.[343] This finding should encourage courts to move away from the analyses in *Arnold* and *Ickes*, as well as *Cotterman*'s acceptance of the search in *Arnold*[344] and *Saboonchi*'s conclusion that manual digital searches are similar to container searches.[345]

Third, *Riley* strongly supports applying the same rule to all digital searches and rejecting distinctions between manual and forensic digital searches. *Riley* consolidated two cases, one involving a smartphone, the other involving a flip phone.[346] The Court could have concluded that the technological differences between smartphones and flip phones should give rise to different standards, because a smartphone generally has more advanced capabilities and could reveal more information than the search of a flip phone.[347] But the Court granted both phones the same Fourth Amendment protection.[348]

The Court also applied a categorical approach—using the same rule for all digital searches—because it is easier for law enforcement to follow and provides greater certainty for individuals.[349] Applying a categorical approach to both exceptions comports better with the Fourth Amendment's particularity element, which requires searches to be limited in scope and tethered to the rationale justifying the initial intrusion.[350] Indeed, the Court rejected several of the government's arguments that officers should be able to search only certain information on a cell phone because such line drawing would be difficult for courts to administer.[351] For example, allowing a search of only information that was potentially pertinent to the reason for arrest "would in effect give 'police officers unbridled discretion to rummage at will among a person's private effects.'"[352] Similarly, allowing officers to search only information they could have searched if there exists a predigital analogue "would launch courts on a difficult line-drawing expedition to

343. *See supra* Part III.B.

344. *See supra* notes 199–201 and accompanying text.

345. *See supra* notes 218–23 and accompanying text.

346. *Riley*, 134 S. Ct. at 2481.

347. *Id.* at 2485.

348. *See id.* (applying the holding to "cell phones," not "smartphones").

349. *See id.* at 2491–92 (noting the Court's "general preference to provide clear guidance to law enforcement through categorical rules. '[I]f police are to have workable rules, the balancing of the competing interests . . . must in large part be done on a categorical basis'" (alterations in original) (citation omitted) (internal quotation marks omitted)).

350. New Jersey v. T.L.O., 469 U.S. 325, 341 (1985).

351. *Riley*, 134 S. Ct. at 2492–93.

352. *Id.* at 2492 (citation omitted).

determine which digital files are comparable to physical records" and "keep defendants and judges guessing for years to come."[353]

Requiring a warrant or reasonable suspicion for forensic digital searches but not manual ones would encourage border officials to manually conduct limitless exploratory digital searches. It would also lead to inconsistent constitutional protections. In a search incident to arrest, police would need a warrant to view the last call someone made on a flip phone. Meanwhile, border officials could manually search through someone's smartphone and laptop computer for hours or even days—so long as it fell short of a forensic search, which could simply mean the use of sophisticated software—just because the owner of the devices took a daytrip to Canada.[354] As the Ninth Circuit stated in *Cotterman*, "[a] person's digital life ought not be hijacked simply by crossing a border." Finally, while it may be true that a forensic search is more intrusive, *Riley* indicates that a certain threshold of intrusiveness is met once a government official has a person's digital life in hand.[355] Applying different standards to forensic and manual digital searches cuts against the Court's logic in *Riley*, neglects the privacy harms of a manual search, and is unworkable.[356]

Courts should also consider the burdens on individuals, who have a legitimate expectation of privacy in their digital information.[357] Anyone who wishes to keep digital information secure would be wise to encrypt everything, which still does not eliminate the risk of confiscation, or simply refrain from traveling internationally with cell phones, laptops, and tablets.[358] But the rapid adoption of electronic devices and frequent travel with them suggest that society is not ready to accept that kind of limit.[359] *Riley*'s recognition of this practical reality indicates the Court is not either.[360]

---

353. *Id.* at 2493 (internal quotation marks and citation omitted).

354. United States v. Cotterman, 709 F.3d 952, 965 (9th Cir. 2013).

355. *See id.*

356. *See supra* notes 314–19 and accompanying text; Brief of Amicus Curiae EFF, *supra* note 27, at 15–20 (arguing that a distinction between manual and forensic searches of digital devices is "meaningless and constitutionally unworkable").

357. *See Riley*, 134 S. Ct. at 2488–89.

358. *See* Abidor v. Napolitano, 990 F. Supp. 2d 260, 277 (E.D.N.Y. 2013); Givens, *supra* note 1.

359. *See supra* notes 28–40 and accompanying text.

360. *See Riley*, 134 S. Ct. at 2484 ("[M]odern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.").

2. Governmental Interests

Riley also provides useful guidance for evaluating the government's interests under the balancing test used to determine whether to exempt digital searches at the border from the warrant requirement.[361] It instructs courts to identify the relevant governmental interests as those that make up the traditional rationale for the exception, rather than the broader array of general law enforcement interests the government claims. *Riley* also counsels courts to examine the extent to which compliance with the warrant requirement would burden the government's ability to promote its traditional interests at the border.

The government has a wide range of interests and obligations at the border, but not all of them justify the border search exception. The longstanding rationale for the exception is based on the government's interests in protecting national security, regulating immigration, and preventing the smuggling of people or contraband.[362] The government urges courts to take a much broader view. As justification for suspicionless and warrantless digital searches, CBP and ICE assert interests in general law enforcement.[363] Certainly, CBP and ICE officials are authorized and obligated to carry out a range of responsibilities, including general law enforcement and cooperation with other law enforcement agencies.[364] But the Court has never announced a broad governmental interest in general law enforcement as a rationale for the border search exception.[365]

Given the intrusiveness of digital searches, courts should adhere to the more specific interests the Court has used to justify the exception and resist conflating the statutory authority of border officials with the traditional justifications for the exception. In *Riley*, the Court examined the traditional rationales for the search incident to arrest exception—officer safety and preservation of evidence—not broad interests in law

---

361. *Id.*

362. United States v. Flores-Montano, 541 U.S. 149, 153 (2004); United States v. Ramsey, 431 U.S. 606, 620 (1977) ("The border-search exception is grounded in the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country."); *see supra* Part I.B–C.

363. CBP DIRECTIVE, *supra* note 2, § 5.4.1.2, at 7 (CBP may retain "information relating to immigration, customs, and other enforcement matters" without probable cause or reasonable suspicion); ICE DIRECTIVE, *supra* note 2, § 8.5(1), at 7 ("ICE may retain information relevant to immigration, customs, and other law enforcement matters" without probable cause or reasonable suspicion).

364. *See* Brief of Appellee United States, at 26–27, United States v. Saboonchi, No. 15-4111 (4th Cir. Nov. 18, 2015) (listing statutory authority of border officials).

365. *See generally supra* Part I.B–C.

enforcement or newly asserted governmental interests.[366] At the border there should be some nexus between the search and the interests the Court has recognized as the basis for the exception.

As part of identifying the relevant government interests, courts should identify which interests are at stake in the search. For example, in *Kim*, the court found that the exit search implicated the government's interest in enforcing customs restrictions but not its interests in national security or general law enforcement.[367]

As a contrary example, in its appeal in *Saboonchi* the government argues that "the purposes underlying the border search doctrine apply in full force to searches of electronic media, which can contain contraband (such as child pornography) or material (such as classified information or malware) that, if illicitly transferred beyond our borders, could pose a direct threat to our national security."[368] Courts must be more precise. Certainly, some digital information in the wrong hands could pose a threat to national security—for example, terrorist plans or certain classified information. Child pornography, on the other hand, implicates the right of the government to exclude contraband; it poses no "direct threat" to national security. Whether malware poses a threat to national security likely has more to do with U.S. cybersecurity systems and practices than whether border officials can conduct suspicionless digital searches. In any case, at least in the *Saboonchi* appeal, the government does little to illustrate the extent of these potential threats to national security.[369]

Riley is useful here as well. There, the Court rejected arguments by California and the United States that speculative or unlikely threats should trump such significant privacy interests protected by the Fourth Amendment. California and the United States argued that officers should be able to search a cell phone incident to arrest in case it would alert them to associates of the arrestee heading to the scene.[370] The Court found there was "undoubtedly a strong government interest in warning officers about such possibilities, but neither the United States nor California offers evidence to suggest that their concerns are based on

366. *See* Riley v. California, __ U.S. __, 134 S. Ct. 2473, 2485 (2014) (examining traditional rationales for the search incident to arrest exception); *see supra* notes 240–52 and accompanying text.

367. *See* United States v. Kim, No. 13-cr-00100-ABJ, 2015 BL 134375, at *23–24 (D.D.C. May 8, 2015), *available at* https://cdn.arstechnica.net/wp-content/uploads/2015/05/kimruling.pdf.

368. Brief of Appellee United States, *supra* note 364, at 31–32.

369. *See id.*

370. *Riley*, 134 S. Ct. at 2485.

actual experience."[371] California and the United States also argued that encryption or remote wiping could inhibit officers from preserving evidence.[372] But the Court had "been given little reason to believe that either problem is prevalent."[373] This part of the Court's analysis suggests that, where there are significant individual interests that ordinarily enjoy constitutional protection, the government bears the burden of demonstrating that its interests should prevail.

After identifying the relevant government interests—national security, immigration, and customs—courts should examine how compliance with the warrant requirement would inhibit the government's ability to protect those interests. In *Riley*, the Court analyzed multiple ways in which officers could secure a cell phone incident to arrest, obviating the need for an immediate search to preserve evidence.[374] The Court also noted that other needs—such as securing the scene—suggest that immediately searching a cell phone is a relatively low priority in the ordinary case.[375]

Border searches take place in a comparable context because of the government's ability to regulate the movement of people and goods. For example, even with a warrant requirement for a digital search, border officials could still temporarily detain the device's owner on the basis of reasonable suspicion and investigate further, reducing or eliminating the need for an immediate suspicionless and warrantless digital search.[376] To draw this conclusion is not to belittle the government's interests at the border, which are significant. Rather, it is simply to point out that, in assessing the burden on the government, courts should examine whether it is necessary for the government to conduct suspicionless digital searches to promote its traditional border interests.

Courts should also pay attention to the practical realities of the border context when assessing potential burdens on the government. Given the millions of travelers carrying electronic devices, border officials lack the resources to conduct widespread suspicionless and warrantless digital

371. *Id.*

372. *Id.* at 2486.

373. *Id.*

374. *Id.* at 2486–88.

375. *Id.*

376. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985) (holding that temporary seizure of individual seeking entrance to the United States was justified by reasonable suspicion that she was smuggling cocaine in her alimentary canal); *cf.* Almeida-Sanchez v. United States, 413 U.S. 266, 291 (1973) (describing the government's power to exclude noncitizens).

searches.[377] They must prioritize. Requiring reasonable suspicion for digital searches is likely to impose minimal burdens on existing practice.[378] As DHS itself acknowledges, "officers very likely do have reasonable suspicion in most searches of electronic devices based on existing screening methods and objective factors."[379] Obtaining a warrant has become simple and fast, taking less than five minutes in some jurisdictions.[380] Moreover, other existing exceptions, such as exigent circumstances, would still apply, providing flexibility to border officials when necessary.[381]

This is not to say that requiring a warrant (or reasonable suspicion) would impose no potential costs in efficiency or convenience to law enforcement. There may be situations where officers have "hard-to-articulate intuitions or hunches" but decline to search an electronic device because there are no objective indications of suspicion.[382] But the Court in *Riley* expressed skepticism about speculative or unlikely reasons for departing from the warrant requirement when such significant individual interests are at stake. And requiring a warrant would hardly put digital information out of reach. Under a probable cause standard border officials would only need to demonstrate there is a "fair probability"[383] that an electronic device contains evidence relating to national security interests or potential immigration or customs violations, or that the individual searched threatens the government's national security interests or seeks to violate immigration or customs laws. A reasonable suspicion standard would require even less.[384] Moreover, the warrant requirement is "an important working part of our machinery of government," not merely "an inconvenience to be somehow 'weighed' against the claims of police efficiency."[385]

---

377. *See* United States v. Cotterman, 709 F.3d 952, 967 n.14 (9th Cir. 2013); U.S. DEP'T OF HOMELAND SEC., *supra* note 42, at 4.

378. *See* Abidor v. Napolitano, 990 F. Supp. 2d 260, 282 (E.D.N.Y. 2013).

379. U.S. DEP'T OF HOMELAND SEC., *supra* note 42, at 17.

380. *See* Missouri v. McNeely, __ U.S. __, 133 S. Ct. 1552, 1573 (2013) (Roberts, C.J., concurring in part and dissenting in part).

381. *See* Riley v. California, __ U.S. __, 134 S. Ct. 2473, 2485 (2014).

382. *See* U.S. DEP'T OF HOMELAND SEC., *supra* note 42, at 17.

383. *See* Safford Unified Sch. Dist. No. 1 v. Redding, 557 U.S. 364, 371 (2009).

384. *See* United States v. Cotterman, 709 F.3d 952, 966 n.14 (9th Cir. 2013) (defending the reasonable suspicion requirement as a "modest, workable standard").

385. *Riley*, 134 S. Ct. at 2493 (citation omitted).

3. Digital Border Searches After Riley

Cotterman, *Saboonchi*, and *Kim* each made significant contributions to the debate over digital border searches. But the debate should develop further. *Riley* supports reexamining whether to apply the border search exception to digital searches. Given the Supreme Court's conclusion that digital searches can be more intrusive than the search of a home, and are fundamentally different from searches of a person or physical property, courts could reasonably conclude under *Riley*'s balancing test that the exception does not apply. In that case, they must revert to the warrant requirement, unless some other exception applies.

But even if courts conclude that the exception does apply, there are two main reasons why they should require either probable cause or reasonable suspicion.

First, *Riley*'s recognition of the intrusiveness of digital searches and its categorical distinction between digital and physical searches indicate that courts should treat digital searches as nonroutine.[386] *Riley*'s application of the same protection to flip phones and smartphones, as well as its preference for a categorical rule, weigh in favor of applying the same rule for all digital searches and doing away with the distinction between manual and forensic searches.[387] Moreover, *Arnold* and *Ickes* are based on reasoning that is flawed in light of *Riley*.[388] The Ninth and Fourth circuits are free to reject those decisions after *Riley* and at least extend the reasonable suspicion requirements in *Cotterman* and *Saboonchi* to all digital searches.

Second, after concluding that digital searches are nonroutine, courts should also consider whether to require probable cause, which will require a similar form of the balancing test under *Riley*. Although the debate over digital border searches has focused on reasonable suspicion, the Supreme Court has never stated or held that all nonroutine searches can be justified by that standard. Rather, it has expressly reserved the question as to the appropriate level of suspicion.[389] Lower courts have generally required reasonable suspicion for nonroutine searches, rather than probable cause, but they have defined nonroutine searches by their level of intrusiveness.[390] *Riley*'s recognition of the unique intrusiveness

386. *See supra* notes 115–25 and accompanying text (discussing intrusiveness as the quality that marks a nonroutine border search).

387. *See supra* notes 349—53.

388. *See supra* Part III.B.

389. *E.g.*, United States v. Montoya de Hernandez, 473 U.S. 531, 541 n.4 (1985).

390. *See supra* notes 115–25 and accompanying text.

of a digital search supports a probable cause standard.

CONCLUSION

Every year, millions of people travel into and out of the United States with a cell phone, tablet, laptop, or some other electronic device. These travelers routinely carry massive amounts of private and confidential information, from personal correspondence to health or banking information, intellectual property, attorney-client documents, and location information. This information may be stored locally, on the device, or on remote servers, in the cloud.

U.S. border officials search and seize digital information without any suspicion of criminal activity, on the proposition that digital searches are no different from physical ones. Until recently, federal courts have accepted this view. The Ninth Circuit and one federal district court have required border officials to demonstrate reasonable suspicion before conducting a forensic digital search. But these decisions still permit intrusive digital searches that fall short of a "forensic" search, and impose only the lowest Fourth Amendment standard.

Riley should lead to significant changes in the digital border search doctrine. Courts should reconsider whether to extend the border search exception to digital searches, drawing on *Riley*'s balancing test. *Riley* supports the conclusion that digital searches—which can be even more intrusive than the search of one's home—fall outside the scope of the border search exception, which is traditionally justified by the government's interest in preventing unwanted people and contraband from entering the country. But even if courts find the border search exception applies, *Riley* should lead them to treat digital searches as nonroutine searches requiring reasonable suspicion or probable cause.