RESTORING PRIVACY AT THE BORDER: EXTENDING THE REASONABLE SUSPICION STANDARD FOR LAPTOP BORDER SEARCHES

Benjamin J. Rankin*

I. INTRODUCTION

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects."[1] In the usual case, a "reasonable" search or seizure is one that is based on probable cause and executed through a judicial warrant.[2] However, the Supreme Court has recognized certain types of searches and seizures as *per se* valid even in the absence of probable cause or a warrant.[3] Under the so-called "border search" exception, the Court has held that warrantless searches of persons or property entering or leaving the country are reasonable simply because of the fact that they occur at the border.[4] As a result, customs officials today have plenary authority to seize and search the property of all travelers entering or exiting the country. No warrant, probable cause, or reasonable suspicion of criminal activity is required.[5]

One of the more controversial questions in this area is how the border search exception should apply to laptop computers. Civil

---

* J.D. Candidate 2012, Columbia Law School. I would like to thank Professor Daniel C. Richman for his invaluable guidance over the better part of a year as I developed this Note. I am also grateful to the superb editors and staff of the *Columbia Human Rights Law Review* for their diligence in editing this piece, and to my parents for their enduring support.

1. U.S. Const. amend. IV.

2. *See, e.g.*, Payton v. New York, 445 U.S. 573, 586–87 (1980) ("It is a 'basic principle of Fourth Amendment law' that searches and seizures inside a home without a warrant are presumptively unreasonable") (quoting Coolidge v. New Hampshire, 403 U.S. 443, 477 (1971)).

3. *Warrantless Searches and Seizures*, 39 Geo. L.J. Ann. Rev. Crim. Proc. 43, 117 (2010).

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

5. *Warrantless Searches and Seizures*, *supra* note 3, at 118.

libertarians argue that laptop border searches implicate greater privacy concerns than searches of other containers, and therefore a heightened standard of suspicion should be required.[6] Yet, in 2008, the Ninth Circuit rejected these claims in *United States v. Arnold*, affirming the authority of customs officials to search laptops entering the country without any suspicion of wrongdoing.[7] Though controversial at the time, the decision in *Arnold* reflects the current status quo, as all federal appellate courts that have addressed the issue agree that reasonable suspicion is not required for searches of laptop computers at the border.[8] On the legislative front, Congress has also failed to enact several proposals that would have required heightened suspicion for such searches.[9]

Backed by the apparent consensus for *Arnold*, the Bush and Obama administrations have embraced the holding in that case as part of current border policy. In July 2008 and August 2009, Customs and Border Protection (CBP) and Immigrations and Customs Enforcement (ICE) each released policy statements expressly endorsing *Arnold*'s rule that no suspicion is required for laptop border searches.[10] In fact, these directives even permit officials to make a full digital copy of a traveler's hard drive and retain it for an indefinite duration.[11] Department of Homeland Security (DHS) records obtained through the Freedom of Information Act confirm that CBP has taken full advantage of these policies. Indeed, between October 2008 and

---

6. *See infra* notes 85–90, 107–11 and accompanying text.

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

8. Yule Kim, Cong. Research Serv., RL 34404, Border Searches of Laptop Computers and Other Electronic Storage Devices 2 (2009) (stating that federal appellate courts that have addressed the degree of suspicion required for laptop border searches "appear to have concluded that reasonable suspicion is not needed to justify such a search").

9. *See, e.g.*, Border Security Search Accountability Act of 2009, H.R. 1726, 111th Cong. (2009) (requiring that the Secretary of Homeland Security issue rules with respect to border security searches of electronic devices); Securing Our Borders and Our Data Act of 2009, H.R. 239, 111th Cong. (2009) (establishing "reasonable suspicion standard" for border security searches of electronic devices and digital storage media); Travelers' Privacy Protection Act of 2008, S. 3612, 110th Cong. (2008) (establishing "reasonable suspicion standard" as applicable to border searches by Homeland Security officers); Electronic Device Privacy Act of 2008, H.R. 6588, 110th Cong. (2008) (precluding searches of laptops and similar devices at the border based on the government's power as sovereign).

10. *See infra* notes 91–100 and accompanying text.

11. *Id.*

June 2010, customs officials searched the electronic devices of 6,671 travelers, nearly half of them American citizens.[12]

In the wake of *Arnold*'s statement of the law and its endorsement by the current administration, several questions arise. How far does the government's laptop border search authority extend? Are there any limitations on the scope of these searches? At what point would *Arnold*-based policies conflict with the Supreme Court's few notable border search decisions?

In the last two years, federal courts have begun to answer these questions, while at the same time establishing new wrinkles in the legal debate over the constitutionality of laptop border searches. In each of these cases, customs officials seized a laptop computer at the border during a border crossing, but then transported the computer to an off-site location—sometimes hundreds of miles away—for a full forensic search.[13] When the defendants filed motions to suppress the evidence as the fruit of warrantless, suspicionless, and illegal searches, the government claimed the searches were "routine," requiring no suspicion at all.

This new class of laptop searches—involving seizures at the border, but searches elsewhere—fell outside of *Arnold*, and thus raised new questions as to how far the suspicionless standard should extend. At least initially, the reaction by federal courts was not favorable to the government. Between 2009 and 2011, four district courts across two circuits held that the extended searches in these cases were lawful under the Fourth Amendment only if officers acted with "reasonable suspicion" of criminal activity—that is, a "particularized and objective" basis for seizing and searching one's laptop.[14] In light of the fact that each court required the government to show heightened suspicion to justify the searches, these decisions appeared to demonstrate a judicial rejection of the government's growing border search authority.

Yet, whatever consensus may have existed among the district courts, the Ninth Circuit Court of Appeals has since stepped in and stopped the trend. In March 2011, the Ninth Circuit reversed a

---

12. *See* David K. Shipler, *Can You Frisk a Hard Drive?*, N.Y. Times, Feb. 20, 2011, at 5 (Week in Review); Press Release, Am. Civil Liberties Union, Groups Sue over Suspicionless Laptop Search Policy at the Border (Sept. 7, 2010), *available at* http://www.aclu.org/free-speech-technology-and-liberty/groups-sue-over-suspicionless-laptop-search-policy-border.

13. *See infra* Part II.A–B.

14. United States v. Montoya de Hernandez, 473 U.S. 531, 541–42 (1985).

district court decision that held that a laptop search occurring 170 miles from the border and two days after the initial border crossing was an "extended border search" requiring heightened suspicion.[15] Rejecting this approach, a two-to-one majority on the Court of Appeals found "no basis under law" to require heightened suspicion for searches in which "some property presented for entry—and not yet admitted or released from the sovereign's control," must "be transported to a secondary site for adequate inspection."[16]

In critiquing the Ninth Circuit's decision, this Note proposes that the laptop searches involved in this recent line of cases represent a *sui generis* category of searches that raises new considerations about the proper limits of the government's border search authority. First, the manner in which these latter searches have been conducted evinces a more wide-ranging, general nature than in previous examples. In earlier laptop search cases, customs officials stationed at the border would search the computer by manually clicking through the desktop, media folders, and internet history to identify evidence of illegal activity.[17] By contrast, in this more recent variety of off-site searches, trained forensic analysts conducted a comprehensive examination of the computer—copying, scanning, and analyzing the entire hard drive—to locate any incriminating evidence.[18] By definition, these new sorts of searches are considerably more invasive, and therefore implicate greater privacy interests for all international travelers. Second, the fact that the government is conducting these latter searches further inland and well after the owner's actual border crossing raises new questions about the reach of the government's border search authority. With these distinctions in mind, the district courts hearing these cases have rightly rejected the government's proposed analogies to *Arnold*, which involved a fundamentally different type of search. Instead, because an off-site forensic search of a laptop computer is both more intrusive and less reasonable in scope than a "routine" border search, district courts have properly analyzed the government's conduct using heightened standards.

Part II lays the legal groundwork for this discussion, beginning with the Fourth Amendment and border search exception,

---

15. United States v. Cotterman, 637 F.3d 1068, 1070 (9th Cir. 2011).

16. *Id.*

17. *See e.g.*, United States v. Arnold, 553 F.3d 1003, 1005 (9th Cir. 2008) (describing a laptop border search that occurred on-site and lasted only a couple of hours).

18. *See infra* notes 104–06, 192–95 and accompanying text.

then focusing more narrowly on laptop searches and extended border searches. Part III introduces the first district court decision—*United States v. Cotterman*[19]—to require reasonable suspicion for off-site laptop searches, and discusses a series of decisions from other courts that adopt its reasoning. Part III also describes the recent Ninth Circuit decision overturning *Cotterman*, and briefly examines this ruling's significance. Part IV begins a critique of recent laptop border search decisions, and defends the *Cotterman* district court decision by explaining how the holding comports with Supreme Court precedent. Finally, Part V examines the policy consequences of requiring heightened suspicion for these particular border searches.

II. THE FOURTH AMENDMENT AND ITS EXCEPTIONS

A. The Border Search Exception

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[20] Under modern Fourth Amendment doctrine, searches and seizures not based on probable cause and executed pursuant to a warrant are presumptively unreasonable and, therefore, unconstitutional.[21]

However, courts have interpreted the Amendment to permit certain types of searches and seizures as exceptions to the probable cause and warrant requirements.[22] Under the "border search"

---

19. United States v. Cotterman, No. CR 07-1207-TUC-RCC, 2009 WL 465028, at *1 (D. Ariz. Feb. 24, 2009), *rev'd* 637 F.3d 1068 (9th Cir. 2011).

20. U.S. Const. amend. IV.

21. *See* United States v. Place, 462 U.S. 696, 701 (1983) (stating that the Court has ordinarily viewed a seizure of personal property as *per se* unreasonable unless it is accomplished pursuant to a warrant based on probable cause); Coolidge v. New Hampshire, 403 U.S. 443, 477–78 (1971) (finding that it is a "basic principle of Fourth Amendment law" that searches and seizures inside a person's house without a warrant are presumptively unreasonable).

22. *See*, *e.g.*, *Place*, 462 U.S. at 701:

> Where law enforcement authorities have probable cause to believe that a container holds contraband or evidence of a crime, but have not secured a warrant, the Court has interpreted the Fourth Amendment to permit seizure of the property, pending issuance of a warrant to examine its contents, if the exigencies of the circumstances demand it or some other recognized exception to the warrant requirement is present.

exception, government officers may conduct routine searches of persons and things crossing the national border "without first obtaining a search warrant and without establishing probable cause."[23] The foundation for this rule traces back to the original customs statute passed by the First Congress, which exempted border searches from probable cause requirements.[24] To this day, customs agents continue to enjoy broad statutory authority to search vehicles and persons upon entering the country.[25]

The Supreme Court has largely embraced this principle of sovereign prerogative in its constitutional doctrine. The Court formally recognized the border search exception in *United States v. Ramsey*,[26] holding that border searches "are reasonable simply by

---

See also United States v. Ross, 456 U.S. 798, 825 (1982) ("The Fourth Amendment proscribes all unreasonable searches and seizures, and it is a cardinal principle that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject to only a few specifically established and well-delineated exceptions.'") (quoting Mincey v. Arizona, 437 U.S. 385, 390 (1978)).

23. 5 Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment § 10.5(a) (4th ed. 2004); *see also* Klein v. United States, 472 F.2d 847, 849 (9th Cir. 1973) ("The mere entry into the United States from a foreign country provides sufficient justification for a border search."); Alexander v. United States, 362 F.2d 379, 382 (9th Cir. 1966) ("The primary purpose of a border search is to seize contraband property sought to be brought into the country."). Some other exceptions include searches incident to arrest, see Chimel v. California, 395 U.S. 752, 762–63 (1969), consent searches, see Zap v. United States, 328 U.S. 624, 630 (1946), and searches of property in plain view, see *Coolidge*, 403 U.S. at 465. For an illustrative list of exceptions, see Craig M. Jackson, *Two Models of the Fourth Amendment*, 83 Mich. L. Rev. 1468, 1473–74 (1985).

24. *See* Act of July 31, 1789, ch. 5, 1 Stat. 29, 43 (1789).

25. *See* 19 U.S.C. § 482(a) (2006).

26. United States v. Ramsey, 431 U.S. 606 (1977). Though this was the first case in which the Court endorsed the border search exception explicitly, it had previously suggested its support for such an exception in dicta. *See* Carroll v. United States, 267 U.S. 132, 154 (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."); United States v. Thirty-Seven Photographs, 402 U.S. 363, 376 (1973) ("[A] port of entry is not a traveler's home. His right to be let alone neither prevents the search of his luggage nor the seizure of unprotected, but illegal, materials when his possession of them is discovered during such a search."); United States v. 12 200-ft. Reels of Super 8mm. Film, 413 U.S. 123, 125 (1973) (finding that border searches, unlike other types of searches, derive their authority from the Commerce Clause, and therefore rest on "different considerations and different rules of constitutional law from domestic regulations. . . . Historically such broad powers have been necessary to prevent smuggling and to prevent prohibited articles from entry.").

virtue of the fact that they occur at the border."[27] In *Ramsey*, a customs official opened international mail without first obtaining a search warrant, based on his observation that the envelopes were "rather bulky" and sent from Thailand, "a known source of narcotics."[28] The Court upheld the search, citing the "long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country . . . ."[29]

While *Ramsey* affirmed that border searches remain free of normal Fourth Amendment requirements,[30] the Court has signaled that more intrusive searches of persons or property are lawful only where government agents act based on a heightened suspicion of wrongdoing. The Court first addressed this issue in *United States v. Montoya de Hernandez*, in which customs officials detained a woman traveling on a direct flight from Colombia based on suspicion that she was a "balloon swallower" attempting to smuggle narcotics into the country by storing them in her alimentary canal.[31] After sixteen hours of detention, the woman was subjected to a court-ordered rectal examination that produced a balloon containing a foreign substance.[32]

In considering what level of suspicion was required for the search, the Court first reaffirmed that Congress had granted the executive branch "plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country."[33] The Court also explained that the "Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior," such that "[r]outine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant . . . ."[34] Still, the Court recognized that "[b]alanced against the sovereign's interests at the border are the Fourth Amendment rights of respondent," with the balance "struck much more favorably

---

27. *Ramsey*, 431 U.S. at 616.
28. *Id*. at 609.
29. *Id*. at 616.
30. The Court reaffirmed *Ramsey* two years later in *Torres v. Puerto Rico*, 442 U.S. 465, 472–73 (1979), finding that "[t]he authority of the United States to search the baggage of arriving international travelers is based on its inherent sovereign authority to protect its territorial integrity."
31. United States v. Montoya de Hernandez, 473 U.S. 531, 533–34 (1985).
32. *Id*. at 535.
33. *Id*. at 537.
34. *Id*. at 538.

to the Government at the border."[35] Using this balancing approach, the Court held that "the detention of a traveler at the border, beyond the scope of a routine customs search and inspection, is justified at its inception if customs agents, considering all the facts surrounding the traveler and her trip, reasonably suspect that the traveler is smuggling contraband in her alimentary canal."[36]

Montoya de Hernandez suggests, then, that some types of border searches—those beyond the scope of a routine customs search and inspection—require a higher level of cause ("reasonable suspicion") to be legally valid. In practice, this holding presents several difficult questions. First, "reasonable suspicion" is a notoriously flexible standard, and a relatively undeveloped area of the law, even today. In past cases, the Court has described it as a level of suspicion lower than probable cause, but has avoided specifying exactly what facts are required to meet the standard.[37] In *Montoya de Hernandez*, for instance, the Court defined the standard, rather unhelpfully, as a "particularized and objective basis for suspecting the particular person" of criminal activity.[38]

Second, the *Montoya de Hernandez* Court refused to identify the categories of border searches in which reasonable suspicion is required. In dicta, the majority explicitly declined to decide "what level of suspicion, if any, is required for non-routine border searches such as strip, body cavity, or involuntary x-ray searches."[39] More recently, lower federal courts have seized on the "routine" and "non-routine" language as distinguishing two separate types of searches with different constitutional requirements.[40] At present, the common

---

35. *Id*. at 539–40.

36. *Id*. at 541.

37. *See* Terry v. Ohio, 392 U.S. 1, 20–21 (1968) (explaining that reasonable suspicion exists where an officer can "point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion").

38. *Montoya de Hernandez*, 473 U.S. at 541.

39. *Id*. at 541 n.4.

40. *See* Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. Rich. L. Rev. 1091, 1102–03 (2009) (asserting that there are two types of border searches: routine searches, which are not subject to any requirement of reasonable suspicion or probable cause, and non-routine searches, which require reasonable suspicion); Sara M. Smyth, *Searches of Computers and Computer Data At the United States Border: The Need for a New Framework Following* United States v. Arnold, 2009 U. Ill. J.L. Tech. & Pol'y 69, 73–75 (2009) (explaining that whether a search is routine or non-routine is the "threshold question" for determining the suspicion required); Kim, *supra* note 8, at 5.

wisdom is that *Montoya de Hernandez* holds that reasonable suspicion is required only for "non-routine" border searches that are similarly intrusive or invasive as the search in this case.[41]

The Supreme Court returned to the question of when reasonable suspicion is required for border searches in *United States v. Flores-Montano*, in which customs officials seized thirty-seven kilograms of marijuana from the defendant's car by removing and disassembling his gas tank.[42] In a unanimous opinion reversing the Ninth Circuit, the Supreme Court held that reasonable suspicion was not required for searches of vehicles at the border.[43] Contrasting this case with *Montoya de Hernandez*, Chief Justice Rehnquist's majority opinion explained that "the 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."[44] In so ruling, the Court reaffirmed the federal government's plenary power at the international border, where the "Government's interest in preventing the entry of unwanted persons and effects is at its zenith."[45]

Still, despite the summary tone with which the Court reaffirmed the government's border search authority, the majority opinion once again left some key questions unanswered. First, the Court declined to answer "whether, and under what circumstances, a border search might be deemed 'unreasonable' because of the particularly offensive manner in which it is carried out."[46] Second, the Court left open the possibility "that some searches of property are so destructive as to require" reasonable suspicion.[47] At any rate, the Court remained silent on what sort of "offensive" or "destructive" searches might meet either test.

B. Traditional Contours of the "Extended Border Search"

While the name of the border search exception may suggest that it only applies to searches at the physical border, in fact the

---

41. *See* Sales, *supra* note 40, at 1103–05; *Warrantless Searches and Seizures*, *supra* note 3, at 119–20.
42. United States v. Flores-Montano, 541 U.S. 149 (2004).
43. *Id*. at 152–53.
44. *Id.* at 152.
45. *Id.*
46. *Id.* at 154–55 n.2 (citing United States v. Ramsey, 431 U.S. 606, 618 (1977)).
47. *Flores-Montano*, 541 U.S. at 155–56.

doctrine is not so limited. Searches occurring away from the border or after an initial border crossing may still avoid normal Fourth Amendment requirements under either of two principles: (1) the "functional equivalent" of the border or (2) the "extended border search."

Searches occurring at a traveler's final port of entry or the first practical detention point after a border crossing are considered to take place at the "functional equivalent" of the border, and therefore require no warrant or suspicion.[48] In *Almeida-Sanchez v. United States*, the Supreme Court found that searches of international passengers arriving at American airports qualify as border searches under this rule.[49]

A second variation on the border search doctrine is the "extended border search." Under this rule, a search taking place *after* an individual has crossed the border may be reasonable if: (1) there is "reasonable certainty" or a "high degree of probability" that the individual crossed a border; (2) there is "reasonable certainty" that the object to be searched has not changed since the border crossing; and (3) there is "reasonable suspicion" that the individual is engaged in criminal activity.[50] Most importantly, unlike regular border searches, extended border searches are valid only when supported by reasonable suspicion.[51]

The Ninth Circuit addressed the heightened suspicion required for extended border searches in *United States v. Alfonso*, in which federal agents conducted an initial cursory search of a ship upon its arrival to Los Angeles Harbor, and then conducted a second search thirty-six hours later that recovered evidence of narcotics trafficking.[52] The Court of Appeals found that the second search was an "extended border search" because of the time lapse between the

---

48. *Warrantless Searches and Seizures*, *supra* note 3, at 120–21.

49. Almeida-Sanchez v. United States, 413 U.S. 266, 273 (1973). For additional examples of searches taking place at the functional equivalent of the border, see *id.* at 272–73.

50. *Warrantless Searches and Seizures*, *supra* note 3, at 121. In the Ninth Circuit, courts eschew the three-part test in favor of a totality of circumstances approach, though reasonable suspicion is still required. *See id*. at 121 n.314; United States v. Sahanaja, 430 F.3d 1049 (9th Cir. 2005).

51. *See, e.g.*, United States v. Cardenas, 9 F.3d 1139, 1148 (5th Cir. 1993) (requiring reasonable suspicion of criminal activity for a constitutional extended border search); United States v. Yang, 286 F.3d 940, 946–47 (7th Cir. 2002) (finding that extended border searches are non-routine and hence must at least be supported by reasonable suspicion).

52. United States v. Alfonso, 759 F.2d 728, 731–33 (9th Cir. 1985).

searches.[53] The court explained that because "[e]xtended border searches occur after the actual entry has been effected and intrude more on an individual's normal expectation of privacy," these searches require "'reasonable suspicion' that the subject of the search was involved in criminal activity, rather than simply mere suspicion or no suspicion."[54] Using this standard, the court upheld the search as valid, finding that the totality of circumstances supported a reasonable suspicion that criminal activity was occurring.[55]

Thus, while *Ramsey*, *Montoya de Hernandez*, and *Flores-Montano* clearly establish that reasonable suspicion is not required for a routine search at the border, the reach of these cases does not extend to those searches that courts deem to be "extended border searches." For this latter type of search, courts have unanimously held that reasonable suspicion is required.

C. The Lay of the Land for Laptop Border Searches

Today, *Ramsey*, *Montoya de Hernandez*, and *Flores-Montano* remain the primary Supreme Court decisions drawing substantive limits on the border search power.[56] Yet, as noted above, these decisions may raise more questions than answers. With such sparse precedent, the Courts of Appeals have been forced to flesh out the contours of the border search exception with little guidance from above.

This is especially true when it comes to border searches of laptop computers, a topic of increasing importance given the ubiquity of the technology among travelers and the obvious privacy interests involved. Laptops today contain massive amounts of personal information about their owners, often carrying "a lifetime of saved email, private photos, passwords, financial and medical records, and evidence of almost any other intimate part of life."[57] As such, obvious

---

53. *Id*. at 734.

54. *Id.*

55. *Id.* at 737. For an illustrative list of cases involving valid extended border searches, see United States v. McGinnis, 247 F. App'x 589, 594 (6th Cir. 2007).

56. *See, e.g.*, United States v. Arnold, 533 F.3d 1003, 1007–08 (9th Cir. 2008) (explaining that *Montoya de Hernandez* and *Flores-Montano* drew "some limits" on the border search power).

57. *Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel: Hearing Before the Subcomm. on the Constitution of the Sen. Comm. on the Judiciary*, 110th Cong. 1 (2008)

questions arise as to how traditional Fourth Amendment principles should apply to this relatively new technology. Yet, to this day, the Supreme Court has still not "decided a single case on when and how the police can search a computer."[58] Such reluctance by the Court has engendered continuing debate among the Courts of Appeals.[59]

The Fifth Circuit first addressed the level of suspicion required for laptop border searches in *United States v. Roberts*.[60] In *Roberts*, customs agents searched a passenger's luggage as he entered a jetway for an international flight, based on information that he usually carried child pornography on diskettes when traveling.[61] The Court of Appeals held that customs agents may conduct a routine search—one that "does not seriously invade a traveler's privacy"—at either the "international border or its functional equivalent without probable cause, a warrant, or any suspicion to justify the search."[62] The court also found it "well-established" that agents "may conduct 'non-routine' searches at the border or its functional equivalent" where they reasonably suspect the traveler is smuggling contraband.[63] Nonetheless, because the court found that reasonable suspicion existed in this case—and therefore the search was lawful whether routine or non-routine—it declined to specify the level of suspicion required for laptop searches generally.[64]

The Fourth Circuit took up the issue of laptop border searches in *United States v. Ickes*, also declining to require any heightened suspicion for laptop searches.[65] In *Ickes*, customs agents searched the defendant's van as he attempted to enter the United States, seizing a computer and seventy-five disks that were later found to contain

---

[hereinafter Subcommittee Hearing] (statement of Peter Swire, C. William O'Neill Professor of Law, Moritz Coll. of Law, The Ohio State Univ.).

58. Shahid M. Shahudullah, *Federal Laws and Judicial Trends in the Prosecution of Cyber Crime Cases in the United States: First and Fourth Amendment Issues*, 45 Crim. L. Bull. 929, 954 (2009) (citing Orin Kerr, *Search and Seizure in a Digital World?*, Legal Aff. Debate Club Blog (Aug. 8, 2005, 9:06 AM), http://www.legalaffairs.org/webexclusive/debateclub_searchseizure0805.msp).

59. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 532–33 (2005) (noting the "thorny issue" for lower courts in deciding how the Fourth Amendment should regulate searches of personal computers).

60. United States v. Roberts, 274 F.3d 1007 (5th Cir. 2001).

61. *Id.* at 1009.

62. *Id.* at 1011 (internal citations omitted).

63. *Id.* at 1012 (internal citations omitted).

64. *Id.* at 1012, 1017.

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

child pornography.[66] In holding that the agents conducted a lawful border search, the court refused to find that laptop searches were different from searches of any other sort of cargo.[67] The court also rejected the defendant's "far-fetched" claim that the holding would permit the government to search the hard drive of "any person carrying a laptop computer . . . on an international flight," since "[c]ustoms agents have neither the time nor the resources to search the contents of every computer."[68]

The Ninth Circuit entered the debate in *United States v. Romm*, in which customs officials at a Canadian airport detained the defendant for questioning upon discovering that he had a criminal record.[69] A brief search of the defendant's computer revealed several child pornography websites in his internet history.[70] Considering the defendant's motion to suppress on appeal, the Ninth Circuit found that the international airport terminal was the "functional equivalent" of a border, and that "passengers deplaning from an international flight are subject to routine border searches."[71] Citing *Montoya de Hernandez*, the court explained that "[u]nder the border search exception, the government may conduct routine searches of persons entering the United States without probable cause, reasonable suspicion, or a warrant."[72] In conclusion, citing *Ramsey*, the court held that the routine border search of the laptop was reasonable "simply by virtue of the fact that [it occurred] at the border."[73]

Taken together, *Romm*, *Roberts*, and *Ickes* all stand for the proposition that customs officials can search laptop computers crossing the border without any suspicion of criminal activity. In these cases, at least, courts have assumed that laptops are no different from other types of containers when it comes to Fourth Amendment restrictions.

---

66. *Id.* at 502–03.

67. *Id.* at 504–05 (citing 18 U.S.C. § 1581(a) (2000) ("Any officer . . . may at any time go on board of any vessel or vehicle at any place in the United States . . . [and search the vehicle] . . . and any person, trunk, package or cargo on board . . . .").

68. *Ickes*, 393 F.3d at 506–07.

69. United States v. Romm, 455 F.3d 990, 994 (9th Cir. 2006).

70. *Id.*

71. *Id.* at 996.

72. *Id.*

73. *Id.* at 997 (citing United States v. Flores-Montano, 541 U.S. 149, 152–53 (2004)) (quoting United States v. Ramsey, 431 U.S. 606, 616 (1977)).

Still, if *Romm* left any ambiguities as to the Ninth Circuit's position, the Court of Appeals decisively answered those questions in *United States v. Arnold*, which expressly held that reasonable suspicion is not required for a warrantless laptop border search.[74] In this case, CBP officials randomly selected the defendant for secondary questioning as he was waiting to pass through customs at an international airport.[75] The officials instructed the defendant to boot up his laptop, then clicked through several folders on his desktop that contained photos of nude women.[76] A more extensive search of his computer over the next several hours revealed images believed to depict child pornography.[77] The officials then seized the computer and obtained a warrant two weeks later to conduct a full search.[78] The District Court for the Central District of California later suppressed all evidence retrieved from the laptop, holding that reasonable suspicion was necessary to conduct the search.[79]

The Court of Appeals reversed, holding that "reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border."[80] The court also refused to analogize to *Flores-Montano*, describing that case as only requiring a higher level of suspicion for "intrusive searches of the person," not his property.[81] Further, the court declined to consider whether the laptop search was "non-routine," explaining that the Supreme Court had discarded the routine/non-routine framework in *Flores-Montano*.[82]

The court also explained that though *Flores-Montano* left open the possibility of requiring reasonable suspicion for "destructive" or "particularly offensive" border searches, neither category applied to the search of Arnold's laptop.[83] The court concluded that "[w]hatever 'particularly offensive manner' might mean, this search certainly does

---

74. United States v. Arnold, 533 F.3d 1003 (9th Cir. 2008).
75. *Id.* at 1005.
76. *Id.*
77. *Id.*
78. *Id.*
79. *Id.* at 1006.
80. *Id.* at 1008.
81. *Arnold*, 533 F.3d at 1007 (paraphrasing the holding in *Montoya de Hernandez*, the court explained that reasonable suspicion is required to search a traveler's alimentary canal because "[t]he interests in human dignity and privacy which the Fourth Amendment protects forbid any such intrusion [beyond the body's surface] on the mere chance that desired evidence might be obtained").
82. *Id.* at 1007.
83. *Id.* at 1007–09.

not meet that test. Arnold has failed to distinguish how the search of his laptop and its electronic contents is logically any different from the suspicionless border searches of travelers' luggage that the Supreme Court and we have allowed."[84] At least for the Ninth Circuit, then, the reasonableness of the laptop search was not open to challenge under the Supreme Court's dicta in earlier border search cases.

D. The Government's Expanding Border Search Authority After *Arnold*

Arnold has been the subject of widespread criticism since the day it was announced.[85] In June 2008, the Senate Judiciary Subcommittee on the Constitution held a hearing on "Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel," focusing primarily on the government's authority to conduct warrantless laptop searches at the border after *Arnold*.[86] One of the major points of contention was the government's argument in *Arnold* that laptops are no different from other types of closed containers, and therefore no heightened suspicion is required for their search.[87] In his testimony, Professor Peter Swire called this a "simplistic legal theory" that "ignores the massive factual differences between a quick glance into a suitcase

---

84. *Id.*

85. For a useful overview of the legal commentary on and criticism of *Arnold*, see Rachel Flipse, *An Unbalanced Standard: Search and Seizure of Electronic Data Under the Border Search Doctrine*, 12 U. Pa. J. Const. L. 851, 861–69 (2010); Ari B. Fontecchio, Note, *Suspicionless Laptop Searches Under the Border Search Doctrine: The Fourth Amendment Exception That Swallows Your Laptop*, 31 Cardozo L. Rev. 231, 259–62 (2009); Smyth, *supra* note 40, at 95; *see also* Peter P. Swire, *Proportionality for High-Tech Searches*, 6 Ohio St. J. Crim. L. 751, 758 (2009) (describing searches of laptop computers at the border without individualized suspicion as an emerging controversy, and claiming that the issue had come into "sharp focus" since the Ninth Circuit's decision in *Arnold*); David E. Brodsky et al., *At the Border, Your Laptop is Wide Open*, Nat'l L. J. (July 22, 2008), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202423144224# (describing how *Arnold* has raised new questions for private companies, including whether their travel and computing policies protect confidential data against the risk it will be searched when their employees enter the country); Ellen Nakashima, *Clarity Sought on Electronics Searches: U.S. Agents Seize Travelers' Devices*, Wash. Post, Feb. 7, 2008, at A1 (claiming that the "seizure of electronics at U.S. borders has prompted protests" from travelers, companies, and civil liberties groups).

86. *Subcommittee Hearing*, *supra* note 57.

87. United States v. Arnold, 533 F.3d 1003, 1009–10 (9th Cir. 2008).

and the ability to copy a lifetime of files from someone's laptop, and then examine those files at the government's leisure."[88] Senator Feingold also challenged the analogy between "the search of a suitcase" and "the search of a laptop containing files upon files of photographs, medical records, financial records, e-mails, letters, journals, and an electronic record of all websites visited. The invasion of privacy represented by a search of a laptop differs by an order of magnitude from that of a suitcase."[89] Nonetheless, following *Arnold*, Congress failed to enact several proposals that would have restricted the government's authority to conduct suspicionless border searches.[90]

At the same time, both the Bush and Obama administrations have embraced *Arnold*'s suspicionless standard as part of their own national security programs. In July 2008, DHS[91] announced new border policies that explicitly authorized customs officials to copy data on laptops and other electronic devices without any suspicion of

88. *Subcommittee Hearing*, *supra* note 57 (statement of Peter Swire, C. William O'Neill Professor of Law, Moritz Coll. of Law, The Ohio State Univ.). For Professor Swire, the government's victory in *Arnold* reflects a "timid Fourth Amendment jurisprudence that is allowing [new surveillance techniques] to spread with few limits from the courts." Swire, *supra* note 85, at 751. *See also* Orin S. Kerr, *The Modest Role of the Warrant Clause in National Security Investigations*, 88 Tex. L. Rev. 1669, 1669 (2010) (explaining that, though warrantless seizures are *per* se unreasonable under the Fourth Amendment, subject to only a few well-delineated exceptions, "the opposite is true" in the context of national security law. In fact, "[t]he Warrant Clause plays a role, but only a modest one . . . [T]he Warrant Clause does not play the significant role in the national security investigations that it plays in criminal investigations.").

89. *Subcommittee Hearing*, *supra* note 57 (statement of Sen. Russ Feingold, Member of the S. Comm. on the Judiciary).

90. *See, e.g.*, Border Security Search Accountability Act of 2009, H.R. 1726, 111th Cong. (2009) (requiring the Secretary of Homeland Security to issue a rule with respect to border security searches of electronic devices); Securing Our Borders and Our Data Act of 2009, H.R. 239, 111th Cong. (2009) (imposing requirements with regard to border searches of digital electronic devices and digital storage media).

91. Border security issues implicate two different agencies within DHS: Customs and Border Protection (CBP), responsible for enforcement at the border, and Immigration and Customs Enforcement (ICE), responsible for enforcement in the interior. *See About CBP*, http://www.cbp.gov/xp/cgov/about (last visited Nov. 4, 2011); *ICE Overview*, http://www.ice.gov/about/overview (last visited Nov. 4, 2011); *see also* Robert M. Bloom, *Border Searches in the Age of Terrorism*, 78 Miss. L. J. 295, 300 (2008) (describing the founding of DHS and the reorganization of border security agencies after 9/11).

wrongdoing.[92] A CBP policy statement permitted its officials to "review and analyze the information transported by any individual" crossing the border "absent individualized suspicion."[93] A similar statement from ICE permitted "ICE special agents acting under border search authority to search, detain, seize, retain, and share documents and electronic media consistent with the guidelines and applicable laws set forth herein . . . ."[94] Moreover, since implementing these policies, DHS officials have vigorously opposed requiring heightened suspicion for laptop searches, citing numerous national security concerns.[95]

During the Obama administration, DHS renewed its endorsement of suspicionless laptop border searches and seizures through a new set of CBP and ICE directives.[96] An August 2009 CBP directive on "Border Search of Electronic Devices Containing Information" stated that "[i]n the course of a border search, *with or without individualized suspicion*, an Officer may examine electronic devices and may review and analyze the information encountered at the border . . . ."[97] The directive also empowered a customs officer to "detain electronic devices, or copies of information therein, for a brief, reasonable period of time," and permitted the search to take place at an "on-site or at an off-site location . . . ."[98] An ICE policy directive from the same month also recognized that "Special Agents acting under border search authority may search, detain, seize, retain, and share electronic devices, or information contained therein, with or without individualized suspicion . . . ."[99] The ICE statement further permitted agents to complete searches of "detained electronic devices, or *copies* of the information therefrom, in a reasonable time."[100]

---

92. *See* U.S. Customs & Border Protection, Policy Regarding Border Search of Information (2008) [hereinafter CBP 2008 Policy]; U.S. Immigration & Customs Enforcement, Directive No. 7-6.0, Border Searches of Documents and Electronic Media (2008) [hereinafter ICE 2008 Policy].

93. CBP 2008 Policy, *supra* note 92, at 1.

94. ICE 2008 Policy, *supra* note 92, at 6.

95. *See infra* notes 226–227 and accompanying text.

96. *See* Ellen Nakashima, *Bush's Search Policy for Travelers is Kept*, Wash. Post, Aug. 28, 2009, at A3.

97. U.S. Customs & Border Protection, CBP Directive No. 3340-049, Border Search of Electronic Devices Containing Information, § 5.1.2 (2009) (emphasis added) [hereinafter CBP 2009 Directive].

98. *Id.* at § 5.3.1.

99. U.S. Immigration & Customs Enforcement, ICE Directive No. 7-6.1, Border Searches of Electronic Devices, § 6.1 (2009).

100. *Id.* at § 8.3(1) (emphasis added).

Compared to the "routine" laptop searches that occurred in *Arnold* and other cases, these policy directives authorize a more comprehensive border search power. As the Court of Appeals described in *Arnold*, the facts of that case involved only a cursory search of the computer's desktop and hard drive by a customs official stationed at the port of entry.[101] The Court of Appeals took care to limit its holding only to this initial search at the actual border.[102] By contrast, CBP and ICE policies authorize a broader set of actions by customs officials—which include seizing any traveler's computer, copying its entire inventory, and retaining the copy indefinitely—all without any suspicion of criminal activity.[103]

As Orin Kerr, Professor of Law at the George Washington University, explains, the forensic searches implicated in these policy statements differ not only in degree from more cursory searches at the border, but also in kind. A full forensic search usually involves an expert analyst "comb[ing] through the world of information inside the computer," using a "range of software programs to aid the search, which can take many days or even weeks to complete."[104] With these tools, the analyst will "sift through the mountain of data in a hard drive and locate specific types or pieces of data" to use in a criminal prosecution.[105] In addition, a forensic search "always begins with the creation of a perfect 'bitstream' copy or 'image' of the original storage

---

101. United States v. Arnold, 533 F.3d 1003, 1005 (9th Cir. 2008) (explaining that ICE agents conducted an examination of the defendant's computer at the airport, lasting no more than a few hours).

102. *Id.* at 1008 (holding that "reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices *at the border*") (emphasis added).

103. A Washington Post article from September 2008 described DHS as "quietly recast[ing]" previous border search policies, which until 2007 generally required agents to have probable cause to suspect criminal activity before copying material a traveler brought into the country. Ellen Nakashima, *Expanded Powers to Search Travelers at Border Detailed*, Wash. Post, Sept. 23, 2008, at A2; *see also* Robert M. Yost, *Deleting Privacy Bit By Bit: An Analysis of* U.S. v. Arnold *and Suspicionless Border Searches of Laptop Computers and Electronic Devices*, 19 Temp. Pol. & Civ. Rts. L. Rev. 303, 304 (2009) (claiming that the *Arnold* decision "grants further deference to [CBP] to promulgate its own policy without judicial input or limitation"); Bloom, *supra* note 91, at 315 (explaining that CBP "elaborated" on its computer search powers after the *Arnold* decision, "allowing for the taking, retaining, copying, and sharing" of information on seized computers, including retention for a "reasonable" time).

104. Kerr, *supra* note 59, at 538.

105. *Id*.

device saved as a 'read only' file," which the analyst retains even after the original computer is returned to the owner.[106]

In short, current federal policy permits the government to seize the computer of any person crossing the national border, make a complete copy of the hard drive, and then search through every file and folder until it discovers something illegal, all without any suspicion of criminal activity. While we may describe this process generically as a "search," it is starkly different from the on-site searches involved in *Arnold* and other previous federal cases.

This subtle expansion of the government's border search authority has prompted a new round of criticism from the legal community, interest groups, and the press. In November 2010, *The New York Times* published a lead editorial claiming that the border search exception "needs updating and tightening to reflect the realities of the digital age," and calling the *Arnold* decision "disappointing."[107] Two months earlier, the American Civil Liberties Union (ACLU) had sued the Department of Homeland Security on behalf of Pascal Abidor, a dual U.S.-French citizen who had his laptop seized at the Canadian border while traveling home to New York.[108] When CBP officials returned Abidor's laptop eleven days later, there was evidence that many of his personal files had been searched.[109] In support of its claim that the CBP and ICE border search policies violated the First and Fourth Amendments, the ACLU complaint cited data obtained through the Freedom of Information Act showing that "[b]etween October 1, 2008 and June 2, 2010, over 6,500 people—nearly 3,000 of them U.S. citizens—were subjected to a search of their electronic devices as they crossed U.S. borders."[110] Moreover, the complaint alleged that between July 2008 and June 2009, border agents shared data from travelers' electronic devices with other federal agencies over 280 times.[111]

---

106. *Id.* at 540.

107. Editorial, *Searching Your Laptop*, N.Y. Times, Nov. 16, 2010, at A30.

108. Press Release, Am. Civil Liberties Union, *supra* note 12; Compl. at 7–13, Abidor v. Napolitano, No. CV 10-4059 (E.D.N.Y. filed Sept. 7, 2010).

109. *See* Press Release, American Civil Liberties Union, *supra* note 12; Compl. at 12, *Abidor*, No. CV 10-4059 (E.D.N.Y. filed Sept. 7, 2010).

110. Compl. at 1, 33, *Abidor*, No. CV 10-4059 (E.D.N.Y. filed Sep. 7, 2010).

111. *See Government Data About Searches of International Travelers' Laptops and Personal Electronic Devices*, Am. Civil Liberties Union (Aug. 25, 2010), http://www.aclu.org/national-security/government-data-about-searches-international-travelers-laptops-and-personal-electr.

III. *COTTERMAN* AND PROGENY: MOVING TOWARD REASONABLE SUSPICION

Over the last two years, several federal courts have issued rulings introducing a new dimension to the legal and policy debates surrounding laptop border searches. These cases are different from both traditional border searches, in which the search and seizure both occur at the actual border, and extended border searches, in which the search and seizure both occur at a time or place removed from the initial border crossing. In this new variety of searches, while the initial seizure of the laptop occurs at the border itself, the actual search of the computer occurs elsewhere, usually at an off-site location in the nation's interior. As such, courts hearing these cases must decide whether to treat these searches as traditional border searches (requiring no suspicion) or extended border searches (requiring reasonable suspicion).

In *United States v. Cotterman*, in which customs officials seized a laptop at the national border but then conducted a forensic search at a location 170 miles inland, the District Court for the District of Arizona ruled that the search was an extended border search requiring reasonable suspicion.[112] In the two-year period following that decision, other district courts across two circuits issued rulings that adopted the same approach, with several citing *Cotterman* as support.[113] Importantly, because each court held that the searches were extended border searches, the government was required to demonstrate reasonable suspicion in each case.[114]

Yet just as *Cotterman* seemed to be gaining traction in other circuits, the Ninth Circuit stepped in and reversed the Arizona court. Citing disagreement with the "logic and practicality" of the district court's analysis, a two-to-one Court of Appeals majority held that the off-site search of the defendant's computer was a routine border search requiring no reasonable suspicion.[115] In so holding, the appellate panel instantly restored the rule that reasonable suspicion

---

112. United States v. Cotterman, No. CR 07-1207-TUC-RCC, 2009 WL 465028, at *1 (D. Ariz. Feb. 24, 2009), *rev'd* 637 F.3d 1068 (9th Cir. 2011).

113. *See* United States v. Hanson, No. CR 09-00946 JSW, 2010 WL 2231796, at *4 (N.D. Cal. June 2, 2010); United States v. Stewart, 715 F.Supp.2d 750, 754 (E.D. Mich. 2010); United States v. Laich, No. 08-20089, 2010 WL 259041, at *1 (E.D. Mich. Jan. 20, 2010).

114. *See Stewart*, 715 F.Supp.2d at 752–53; *Hanson*, 2010 WL 2231796 at *4; *Laich*, 2010 WL 259041 at *4.

115. United States v. Cotterman, 637 F.3d 1068, 1070 (9th Cir. 2011).

is not required for laptop border searches in the Ninth Circuit. Other circuits with similar cases will be left to decide whether to follow suit.

A. *United States v. Cotterman* and the New Extended Border Search

In *United States v. Cotterman*, customs officials at the Lukeville, Arizona port of entry found two laptop computers in the defendant's car during a routine border search.[116] Because of the defendant's past convictions for child sex crimes, and the agents' observation that several files on one of the laptops were password-protected, the agents seized both computers.[117] Later that same day, an ICE agent drove the computers to a site in Tucson for a full forensic evaluation.[118] Two days later, a forensic specialist discovered seventy-five images of child pornography on the defendant's laptop.[119] In his subsequent criminal trial, the defendant moved to suppress the images, claiming that the search of his laptop 170 miles from the port of entry over a period of four days was a non-routine border search requiring reasonable suspicion.[120]

The District Court for the District of Arizona rejected the government's analogy to *Arnold*, *Ickes*, *Romm*, and *Roberts*, finding that these cases applied only where "evidence of child pornography was discovered physically at the border within a few hours of examining the laptop."[121] The court then addressed the question of whether the government could "seize property at the border, move it far away from the border and hold the property for days, weeks or months without any heightened scrutiny."[122] Under these circumstances, the court found that the government had conducted an extended border search.[123] The court explained that searches "removed in time and place from the border" represented "a greater

---

116. Cotterman, 2009 WL 465028 at *1–2.
117. *Id.* at *2.
118. *Id.*
119. *Id.* Though agents found no contraband on the second laptop, which belonged to the defendant's wife, the agents made a copy of the laptop and, at the time of the trial, still retained it. *Id.*
120. *Id.* at *3.
121. *Id.*
122. *Id.*
123. *Id.* at *4 ("Under those circumstances, the law requires the Government to have reasonable suspicion before extending the search in both distance and time away from the border.").

intrusion on the person," and were therefore valid only if supported by reasonable suspicion.[124] In conclusion, the court stated that:

> In a border search, time and distance do matter. In the *Alfonso* case, thirty-six hours was too long. Certainly 170 miles is too far. Therefore, based on both extended time and distance the computer forensic search in this case was an extended border search requiring reasonable suspicion of criminal activity before taking the computers away from the port of entry.[125]

Because the search in *Cotterman* took place at a different time and place than the initial seizure at the border, the case does not line up easily with either the traditional border search or the extended border search principles.[126] In fact, the search seems to fall somewhere between the two, since the seizure occurred at the actual border, and the search occurred at an inland site. But the interesting move taken by the district court was to treat this type of search as a full-fledged extended border search, justified only by a showing of reasonable suspicion.[127] In the court's analysis, transporting Cotterman's laptop to a site 170 miles from the border was like conducting a search thirty-six hours after crossing the border; in either case, the extended search represented a greater intrusion on the defendant's rights.

---

124. *Id.* at *4–5.

125. *Id.* at *9.

126. For an insightful discussion of how *Cotterman* is different from traditional border search cases, see Orin S. Kerr, *Does the Border Search Doctrine Apply To Searching Computers if the Government Moves the Computer Away from the Border Before Searching It?*, The Volokh Conspiracy (Mar. 2, 2009, 10:36 PM), http://volokh.com/2009/03/02/does-the-border-search-doctrine-apply-to-searching-computers-if-the-government-moves-the-computer-away-from-the-border-before-searching-it.

127. *See id.* (noting that Ninth Circuit cases "have ruled that as time and space passes from the initial border crossing, a search can be justified based on reasonable suspicion—and that only after more time/space passes from the border is a search no longer even an 'extended border search.'"); *see also* United States v. Stewart, 715 F.Supp.2d 750, 754 (E.D. Mich. 2010) ("The court distinguished cases from other circuits upholding searches of computers on which child pornography was found on the basis of the location of the search (at the point of entry—usually an airport) and the time involved (generally a matter of hours and not days).").

B. *Cotterman* Takes Hold With Other Courts

Cotterman was the first decision to apply an extended border search analysis to off-site searches of laptop computers following a seizure at the border. But its reasoning quickly gained traction with other district courts, both within and outside the Ninth Circuit.

In *United States v. Stewart*, two customs officials searched the defendant's laptop as he passed through inspection at a Detroit airport, discovering several photos that they believed to be child pornography.[128] Because the agents could not access a second laptop in the defendant's luggage, they transported both laptops to the local ICE headquarters twenty miles away for a full forensic search.[129] A search at the off-site location revealed child pornography.[130]

At trial, the defendant claimed that the search of his computer the day after its seizure at another location was an extended border search, citing *Cotterman* as support.[131] The Eastern District of Michigan agreed, holding that the off-site search was an extended border search requiring reasonable suspicion.[132] The court explained that "[r]emoving the laptops from the point of entry into the country and transporting them to a remote forensic laboratory may result in an intrusion greater than one might reasonably expect upon entering or re-entering the United States."[133] Thus, though a person arriving at the border should reasonably expect that her property will be inspected before entry, the "actual dispossession" of a traveler's belongings as occurred in this case is "different in kind from an inspection of those items, however thorough, at the border."[134]

Both *Cotterman* and *Stewart* were cited approvingly by the District Court for the Northern District of California in *United States v. Hanson*, in which customs officials searched the defendant's laptop

---

128. Stewart, 715 F.Supp.2d at 751–52.

129. *Id.* at 752.

130. *Id.*

131. *Id.* at 754 ("The defendant cites *United States v. Cotterman* . . . as an example of a seizure of a computer at a border that ripened into an 'extended border search,' which required reasonable suspicion.").

132. *Id.* at 755. ("The defendant's analogy to the extended border search cases therefore is apt."). However, on the facts of this case, the court found that the agents had reasonable suspicion to believe the computers contained contraband. *Id.*

133. *Id.* at 754.

134. *Id.*

three times over a period of several months, all without a warrant.[135] Following the defendant's arrival at San Francisco International Airport, a customs search of his laptop computer revealed an image of a nude adolescent female.[136] After customs officers sent the laptop to an off-site CBP laboratory, a forensic search recovered further evidence of child pornography.[137] A third search several months later revealed over 1,000 illicit images.[138]

At trial, the government conceded that the second search at the CBP lab was an extended border search, but claimed that reasonable suspicion supported the search.[139] The court analyzed the government's claim by citing *Cotterman*,[140] and concluded that the search was an extended border search due to "the passage of time between the [first two] searches and the fact that the [second] search was not conduct [sic] at the border, or its functional equivalent . . . ."[141] However, the court found that reasonable suspicion justified the search, with the facts of this case "more analogous to *Stewart* than to *Cotterman*."[142]

Another case from the Sixth Circuit also deserves mention, even though the court did not cite *Cotterman* explicitly. In *United States v. Laich*, CBP officials seized the defendant's laptop as he passed through customs at Dallas–Fort Worth International Airport, then shipped the computer to an ICE agent in Detroit.[143] The ICE agent then conducted a warrantless forensic search of the laptop, discovering multiple child pornography images and movies.[144]

---

135. United States v. Hanson, No. CR 09-00946 JSW, 2010 WL 2231796, at *1–2 (N.D. Cal. June 2, 2010).

136. *Id.* at *1.

137. *Id.* at *1–2.

138. *Id.* at *2.

139. *Id.* at *4.

140. *Id.* ("Because the agents did not find contraband while the laptop was located at the border and, in light of the time and distance that elapsed before the search continued, the court concluded that the search should be analyzed as an extended border search.").

141. *Id.*

142. *Id*. at *5. The court ruled against the government on the third search—again citing *Cotterman*—finding that "the discrepancy in time and distance" between the search and the border was "so great that it [was] no longer an extended border search, thus requiring probable cause and a warrant." *Id.*

143. United States v. Laich, No. 08-20089, 2010 WL 259041, at *1–2 (E.D. Mich. Jan. 20, 2010).

144. *Id.* at *2.

Upon finding that customs officials detained the defendant at the border after completing their initial search, the District Court for the Eastern District of Michigan held that the government had conducted an extended border search.[145] Though the court suggested that the initial seizure of the computer may have been justified under the border search exception, it found that the government could not justify a permanent seizure of the laptop unless the defendant "was reasonably suspected of criminal activity related to his border crossing."[146] Without such cause, "the Government's decision to permanently seize Laich's property in Dallas and transport it hundreds of miles to another jurisdiction for further search was unreasonable by Fourth Amendment standards."[147] Here, the court treaded close to adopting the reasoning in *Cotterman*, though it did not cite the decision or base its holding on those same grounds. Still, taken together with *Stewart* and *Hanson*, *Laich* was another example in which a federal court held that reasonable suspicion should be required for certain extended laptop searches.[148]

C. *Cotterman*'s Reversal in the Ninth Circuit

This consensus among the district courts, such as it was, was short-lived. Approximately two years after the District Court of Arizona decided *Cotterman*, a three-judge panel on the Ninth Circuit Court of Appeals reversed in a two-to-one decision.[149] Calling it a case of first impression, Judge Richard Tallman phrased the question presented as "whether the search of a laptop computer that begins at the border and ends two days later in a Government forensic computer laboratory almost 170 miles away can still fall within the

---

145 *Id.* at *3–4.

146 *Id.* at *4.

147. *Id.*

148. The District Court for the Western District of New York also cited *Cotterman* approvingly in United States v. Rogozin, No. 09-CR-379 (S)(M), 2010 WL 4628520, at *1 (W.D.N.Y. Nov. 16, 2010). In that case, ICE agents seized the defendant's laptop computer, video recorder, iPhone, and camera after observing images that they believed contained child pornography, and then searched them at an off-site location at a later date. *Id.* at *1–2. The court found that reasonable suspicion justified the search of the laptop, thereby avoiding the question of whether the search was routine. *Id.* at *3. But the court suppressed all other evidence because the government held it longer than CBP guidelines allowed. *Id.* at *4–5. In this order, the court cited *Cotterman* to support its finding that the court may have to suppress evidence when the government detains property beyond the time needed to search it. *Id.* at *4.

149. United States v. Cotterman, 637 F.3d 1068 (9th Cir. 2011).

border search doctrine."[150] In ruling for the government, the majority rejected the claim that the search was not a typical border search merely because "logic and practicality" required customs officers to transport the computer from the point of entry to a "secondary site for adequate inspection."[151]

In analyzing when the Fourth Amendment requires particularized suspicion, the "touchstone" for the majority's analysis was "the greater Fourth Amendment intrusion that occurs when an individual is detained and searched at a *location beyond the border where he had a normal expectation of privacy in the object searched*."[152] By contrast, Cotterman was detained and searched "at the border itself—a point at which travelers do not have a normal expectation of privacy, but rather must expect to have their privacy intruded upon."[153] Further, because customs officers "made it abundantly clear to Cotterman that his computers and cameras were not cleared for entry" and would not be until they were fully examined, Cotterman "never regained his normal expectation of privacy."[154] Absent this expectation, the Fourth Amendment did not restrict the search and seizure.

Having reached this basic conclusion, the majority went on to challenge the policy implications of the defendant's view of the Fourth Amendment. For the majority, upholding the district court decision presented an impossible dilemma for the government: either the government must furnish every port of entry "with the equipment and personnel needed to fully search all incoming property or otherwise be forced to blindly shut its eyes and hope for the best absent some particularized suspicion."[155] The court refused to endorse such a rule.[156]

As a concession, the majority provided certain limits to its border search exception, "stop[ping] far short of 'anything goes' at the border."[157] As the majority explained, "The Government cannot simply seize property under its border search power and hold it for

---

150. *Id.* at 1070.
151. *Id.*
152. *Id.* at 1076 (citation omitted).
153. *Id.* at 1077.
154. *Id.*
155. *Id.*
156. *See id.* at 1079 ("We flatly reject the contention that the Government must categorically demonstrate reasonable suspicion to continue a search initiated at the border to a secondary site.").
157. *Id.* at 1070.

weeks, months, or years on a whim."[158] Instead, following *Flores-Montano* and *Montoya de Hernandez*, courts should continue to scrutinize border searches on a case-by-case basis, "to determine whether the manner of the search and seizure was so egregious as to render it unreasonable."[159] Finding that the government had conducted a reasonable search in this case, the majority reversed the district court's suppression of evidence.[160]

In dissent, Judge Betty Fletcher challenged the majority's framing of the issue. Instead of focusing on whether the government could transport property from the border to continue a search, Judge Fletcher defined the "sticking point" in the case as "whether the Government has authority *to seize* an individual's property in order to conduct an exhaustive search that takes days, weeks, or even months, with *no reason* to suspect that the property contains contraband."[161] For Judge Fletcher, in light of the "exhaustive nature of computer forensic searches," the Fourth Amendment would only allow such searches where "guided by an officer's reasonable suspicion that the computer contains evidence of a *particular* crime."[162]

In support of this proposition, Fletcher first rejected the claim that the government did not intrude on the defendant's reasonable expectation of privacy. While conceding that "a traveler cannot have a reasonable expectation that his property will not be searched at the border," Fletcher claimed that "a traveler does have a reasonable expectation that his property will not be searched in a manner that requires it to be taken away from him for weeks or months," unless the government has some basis to believe the property contains contraband.[163] As such, in light of the fact that the government did not argue on appeal that CBP officers acted with reasonable suspicion in seizing the laptop, the Court of Appeals should have found a constitutional violation.[164]

---

158. *Id.*
159. *Id.*
160. *Id.*
161. *Id.* at 1084 (Fletcher, J., dissenting).
162. *Id*. at 1086 (Fletcher, J., dissenting).
163. *Id*. at 1085 (Fletcher, J., dissenting) (citation omitted).
164. In its interlocutory appeal to the Ninth Circuit, the government did not claim that reasonable suspicion supported the search. *See id*. at 1074. Rather, the government instead claimed that no reasonable suspicion was needed because both the seizure and subsequent search fell squarely within the regular border search exception. *See, e.g.*, Orin S. Kerr, *Update on United States v. Cotterman, Ninth Circuit Case Applying the Border Search Exception to Computers*, The Volokh Conspiracy (Jan. 17, 2011, 1:38 AM), http://www.volokh.com/2011/01/17/

The crux of Fletcher's dissent is in the final pages, where she speculates on the implications of the majority's rule. Fletcher laments that the court's holding permits the government to seize and search any traveler's computer without justification, and then search inside the computer until agents discover some evidence of criminal activity. She writes, "The majority gives the Government a free pass to copy, review, categorize, and even read all of that information in the hope that it will find *some* evidence of *any* crime."[165] While she concedes that such a policy would permit CBP officers to "ensure that there is no child pornography or information about terrorist plots on the computer," it would also allow officers to

> translate any documents in a foreign language, ensure that none of the seemingly innocuous pictures are actually encrypted messages, verify the licenses on any music or movies on the computer, review financial logs for evidence of insider trading, read email correspondence to ensure that there is no communication with known criminals . . . .[166]

Indeed, "the list of possible 'concerns' is endless, particularly where the Government expressly seeks to use its border search power to uncover evidence of crimes unrelated to contraband smuggling or national security."[167]

D. Relevance of the *Cotterman* District Court Decision Today

In light of the Ninth Circuit's holding, the *Cotterman* district court decision clearly carries no legal authority today. Nonetheless, decisions like *Stewart* and *Laich* survive—for now—as evidence that other jurisdictions favored the logic of the lower court decision. Time will tell whether the argument for reasonable suspicion in these extended laptop searches continues to take hold in other circuits. At least, as discussed in the next section, there are good reasons to

---

update-on-united-states-v-cotterman-ninth-circuit-case-applying-the-border-search-exception-to-computers/ (claiming that the government deliberately declined to argue reasonable suspicion in order to be able to appeal an adverse decision on the governing legal standard to the Supreme Court). The majority declined to challenge the district court's finding that no reasonable suspicion existed. *See Cotterman*, 637 F.3d at 1074 n.7 (noting the district court's finding that "only two facts supported reasonable suspicion: Cotterman was a convicted sex offender on a watch list, and he had password-protected files on his computer.").

165. *Cotterman*, 637 F.3d at 1085–86 (Fletcher, J., dissenting).

166. *Id*. at 1086 n.5 (Fletcher, J., dissenting).

167. *Id*. (citation omitted).

support this continuing extension of the *Cotterman* district court's rule.

IV. DOCTRINAL SUPPORT FOR *COTTERMAN*'S REASONABLE SUSPICION REQUIREMENT

This Note endorses the *Cotterman* district court's holding that reasonable suspicion of criminal activity is required before the government may conduct an off-site forensic search of a laptop computer seized at the border.[168] Indeed, in reversing this decision, the Court of Appeals exhibits a flawed understanding of the Fourth Amendment that offends Supreme Court border search precedent. In Part IV, this Note explains where the Ninth Circuit went wrong, and suggests two reasons why the district court decision better comports with existing federal precedent. First, full forensic searches of personal computers at off-site locations are likely to be more *intrusive* than typical laptop searches conducted at the border. Second, such off-site searches may be unreasonable in *scope* under *Montoya de Hernandez* and *Flores-Montano*. If the scope of laptop searches is to be expanded beyond the more "routine" searches in previous cases, a higher level of suspicion must be required.

A. Off-Site Forensic Searches Are More Intrusive Than Routine Border Searches

The Supreme Court has long recognized that the intrusiveness of a search or seizure is relevant to its reasonableness under the Fourth Amendment. In *Katz v. United States*, Justice Harlan explained the Court's rule for protection under the Fourth Amendment as a two-part test.[169] First, a person must have an actual (subjective) expectation of privacy.[170] Second, this expectation must be one that society recognizes as "reasonable."[171] To illustrate, Harlan explained that searches or seizures in a person's home would be protected (since one has an expectation of privacy there), but conversations taking place in public "would not be protected against being overheard" (since the expectation of privacy would be

---

168. United States v. Cotterman, No. CR 07-1207-TUC-RCC, 2009 WL 465028, at *5 (D. Ariz. Feb. 24, 2009), *rev'd* 637 F.3d 1068 (9th Cir. 2011).

169. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

170. *Id.*

171. *Id.*

unreasonable).[172] Though initially published as a concurrence, Harlan's formulation in *Katz v. United States,* expressly linking the reasonableness of a search to its intrusion on an individual's privacy interests, was embraced in *Smith v. Maryland*.[173]

In the context of searches and seizures conducted without a warrant, or based on less than probable cause, the Court has suggested that the degree of intrusiveness may be linked even more directly to a determination of reasonableness. In *United States v. Place*, the Court considered whether federal agents violated the Fourth Amendment by seizing a passenger's luggage and detaining it for ninety minutes without probable cause.[174] Rejecting the government's proposal for a blanket endorsement of luggage searches and seizures on less than probable cause, the Court found that the reasonableness of such a warrantless seizure depended on balancing the "nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion."[175] Here, the Court strongly suggested that whether a warrantless search or seizure is reasonable under the Fourth Amendment will depend largely on the degree of intrusiveness of the search or seizure.[176] As the Court described, seizures of property can vary in intrusiveness, and "some brief detentions of personal effects may be so minimally intrusive of Fourth Amendment interests that strong countervailing governmental interests will justify a seizure based only on [reasonable suspicion]."[177] In this case, however, the Court found that the length of detention of the defendant's luggage precluded a finding of reasonableness in the absence of probable cause.[178]

---

172. *Id.*

173. *See id.*; Smith v. Maryland, 442 U.S. 735, 740 (1979) (holding that "the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action"); *see also* Orin S. Kerr, *Four Models of Fourth Amendment Protection,* 60 Stan. L. Rev. 503, 504 (2007) (explaining that the Supreme Court has interpreted the Fourth Amendment to regulate conduct that violates an individual's reasonable expectation of privacy); Jed Rubenfeld, *The End of Privacy*, 61 Stan. L. Rev. 101, 105–06 (2008) (describing that the Court adopted Harlan's test not long after *Katz*, and that the Fourth Amendment has been found to protect a "reasonable expectation of privacy" ever since).

174. United States v. Place, 462 U.S. 696, 699–700 (1983).

175. *Id.* at 703.

176. *Id*. at 703–04.

177. *Id*. at 706.

178. *Id*. at 709.

The question of intrusiveness remains important for border searches as well. Indeed, both *Flores-Montano* and *Montoya de Hernandez* suggest that the intrusiveness of a search will be one of the key factors in determining whether a search is routine, requiring no reasonable suspicion, or non-routine, requiring heightened suspicion. In *Flores-Montano*, the Court anticipated that in cases involving "highly intrusive searches of the person," the "*dignity and privacy interests of the person being searched*" might require a higher level of suspicion, even though these interests did not "carry over" to the vehicle search at issue in this case.[179] Similarly, in *Montoya de Hernandez*, the Court described strip, body cavity, and involuntary x-ray searches as "non-routine" border searches, suggesting that other intrusive searches might also require heightened suspicion.[180]

The basic question presented by cases like *Cotterman* is whether an off-site forensic search of a laptop seized at the border is so intrusive—or, so much more intrusive than a search occurring at the actual border, as in *Arnold*—as to require a higher level of suspicion. In response, this Note proposes that off-site forensic searches *are* more intrusive than routine border searches—that they more strongly implicate dignity and privacy interests of the person being searched—and therefore, under the Supreme Court's own tests, reasonable suspicion should be required.

A comparison of routine laptop border searches and off-site forensic searches will help to illuminate the distinction. *Arnold* presents a good example of a "routine" laptop border search. In that case, after CBP agents asked an international traveler to turn on his laptop computer, the officials observed several folders on his desktop containing photos of nude women.[181] In a follow-up search that occurred on-site, ICE agents examined the computer over several hours and found "numerous images" believed to be child pornography.[182] The only question before the Court of Appeals was what level of suspicion was required for these preliminary searches.[183]

---

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

180. United States v. Montoya de Hernandez, 473 U.S. 531, 541 n.4 (1985).

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

182. *Id*.

183. *Id*. ("We must decide whether customs officers at Los Angeles International Airport may examine the electronic contents of a passenger's laptop computer without reasonable suspicion."). It should be noted that though the government conducted a fuller forensic search after seizing the computer, this later search was conducted after the agents obtained a search warrant. *Id*.

Yet, there is a stark difference between the searches and seizures that took place in *Arnold* and *Cotterman*.[184] While ICE agents completed their cursory search of Arnold's computer in only a few hours, in *Cotterman*, a trained forensic specialist took almost two full days to conduct a comprehensive scan of the hard drives belonging to the defendant and his wife.[185] Moreover, the border officials in *Cotterman* retained copies of both the defendant's computer and his wife's, even though a forensic search revealed no contraband on the wife's computer.[186] As such, when these cases are placed side-by-side, there is clearly not much of an option between the search in *Arnold* and the full forensic inventory in *Cotterman*. The *Cotterman* district court—noting the greater intrusiveness of the off-site search—was unwilling to apply the same standard to both.[187]

Some have proposed that laptop searches by customs officers at the border have the potential to be less intrusive than normal searches of property.[188] Professor Nathan Sales notes that in a "standard border search," "customs officers manually rifle through travelers' belongings, personally inspecting every item to determine whether it is contraband or evidence of crime."[189] Sales suggests that CBP officers should instead conduct laptop searches through a "basic keyword search, an automated and impersonal computer process . . . [that] separates the few pieces of data that might have investigative significance from the larger mass of information that has no relevance to the government's counterterrorism or law-enforcement functions."[190] Sales argues that keyword searches are akin to "canine

184. United States v. Cotterman, No. CR 07-1207-TUC-RCC, 2009 WL 465028, at *2 (D. Ariz. Feb. 24, 2009), *rev'd* 637 F.3d 1068 (9th Cir. 2011).

185. *Id.* (noting that the forensic specialist received the equipment at 11 PM on Friday, April 6, 2007 and began the forensic evaluation immediately, and that he continued the examination on Saturday and Sunday); *see also* United States v. Hanson, No. CR 09-00946 JSW, 2010 WL 2231796, at *1 (N.D. Cal. June 2, 2010) (noting that a forensic scientist "systematically checked the contents of the hard drive" for evidence of child pornography).

186. *Cotterman,* 2009 WL 465028, at *2. The court ordered the government to return the copy of Mrs. Cotterman's laptop and to retain no copy of it. *Id*. at *10.

187. *Id.* at *5.

188. Sales, *supra* note 40, at 1119 (claiming that "searches of laptop computers have the potential to be *less*, not more, intrusive than traditional border searches of luggage and cargo").

189. *Id.* at 1119–20.

190. *Id.* at 1120.

sniffs," a less intrusive type of search that avoids unnecessary exposure of one's private property.[191]

But this argument, by definition, does not apply to the comprehensive forensic searches that took place in *Cotterman* and other cases. As Professor Kerr explains, forensic searches typically involve both "logical" data searches—such as the keyword search that Sales proposes—and more extensive "physical" searches.[192] In fact, a logical search "ordinarily does not suffice," forcing the analyst to conduct a physical search of the entire hard drive.[193] As a result, the analyst will view not only the "discrete pieces of data that are flagged in the keyword search," as Sales imagines, but "massive volumes of sensitive personal data," exactly what his proposal was designed to avoid.[194] Without the more targeted laptop search that he proposes, even Sales recognizes the "conventional wisdom" that "border inspections of laptop computers are an especially intrusive kind of search, maybe even rivaling the invasiveness of a strip or body-cavity search."[195]

Still, others might argue that while forensic searches might be more *extensive* than standard border searches, they are not necessarily more *intrusive*, at least as the Supreme Court has defined that term. Some commentators read *Montoya de Hernandez* and *Flores-Montano* as proposing that only searches *of the person*, not of property, may qualify as intrusive under the Court's analysis. One such commentator, Professor Larry Cunningham, claims that courts have "correctly rejected attempts to analogize laptop searches to the type of search and seizure conducted in *Montoya de Hernandez*."[196] As he states, "A laptop computer—no matter the quantity or nature of

---

191. *Id.* at 1122; *see also* United States v. Place, 462 U.S. 696, 699 (1983).

192. *See* Kerr, *supra* note 59, at 544–45.

193. *Id.* at 545.

194. Sales, *supra* note 40, at 1120–22. For more on the amount of personal information typically stored on a laptop, see Kerr, *supra* note 59, at 542 ("Computer hard drives sold in 2005 generally have storage capacities of about eighty gigabytes, roughly equivalent to forty million pages of text—about the amount of information contained in the books on one floor of a typical academic library.").

195. Sales, *supra* note 40, at 1119.

196. *Subcommittee Hearing*, *supra* note 57, at 107 (statement of Larry Cunningham, Assistant Dist. Attorney for Bronx Cnty., Assistant Professor of Legal Writing, St. John's Univ. Sch. of Law) ("The search and seizure in *Montoya de Hernandez* was considered 'non-routine' not just because it was an intrusion into the defendant's privacy. The Court's decision was also based on the fact that there was a unique 'interest[] in human dignity' that was at stake.")

the information contained within it—simply does not implicate the same degree of privacy concerns involved with a person's 'alimentary canal.'"[197]

But, perhaps the correct reading of these cases is to focus on the level of intrusiveness involved in the searches at issue, and not categorical determinations about whether the search involved a person or property. In *Montoya de Hernandez*, when the Court listed strip, body cavity, and involuntary x-ray searches as examples of "non-routine" searches, the salient criterion that made these searches "non-routine" was the level of intrusiveness, not the fact that they involve personal searches. *Montoya de Hernandez* suggests that the Court prefers a sliding-scale approach to intrusiveness, requiring heightened suspicion as the search becomes more intrusive.[198]

If the Court were to apply the same analysis today, it should find that forensic computer searches also demand heightened suspicion. At the time the Court decided *Montoya de Hernandez* in 1985, it could not have contemplated that digital devices in today's world would implicate the same privacy and dignity interests as other personal searches.[199] But that the Court did not foresee this possibility and include "laptop searches" in its list of non-routine searches did not foreclose the possibility that it would find this way in a future case.

Still, if the degree of intrusiveness is the Court's most important criterion in deciding the appropriate level of suspicion for a search, then *Flores-Montano* may seem like a glaring exception. That case presented an opportunity for the Court to establish clearly that all border searches, whether of one's person or property, would be measured according to the degree of intrusiveness involved. Yet, the Court declined that invitation, flatly refusing to consider whether a search of a vehicle might be so "intrusive" as to require heightened suspicion.[200] As such, its holding may be read to stand for the categorical proposition that "extensive, time-consuming, and

---

197. *Id.* at 70.

198. *See, e.g.*, United States v. Vance, 62 F.3d 1152, 1156 (9th Cir. 1995) (asserting that a strip search is intrusive enough to require "real suspicion").

199. *See, e.g.*, *Subcommittee Hearing*, *supra* note 57, at 2 (statement of Sen. Russ Feingold) ("I guarantee you this: neither the drafters of the Fourth Amendment, nor the Supreme Court when it crafted the 'border search exception,' ever dreamed that tens of thousands of Americans would cross the border every day, carrying with them the equivalent of a full library of their most personal information.").

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

potentially destructive warrantless searches" of property do not require any individualized suspicion of wrongdoing.[201]

However, reading *Flores-Montano* to prohibit any searches of property from ever qualifying as "intrusive" would oversimplify the Court's decision. Indeed, the Court expressly limited the holding to the level of suspicion required for the disassembly and removal of the defendant's fuel tank.[202] As such, while an intrusiveness analysis might be appropriate in other cases involving property searches, the Court found it to be inappropriate on the facts presented. As the Court stated in dicta, it was "difficult to imagine" that the "search of a gas tank, which should be solely a repository for fuel," was an unreasonable invasion of privacy under the Fourth Amendment.[203] In contrast, given the obvious privacy interests involved, it should be much less difficult for the Court today to imagine that a forensic laptop search is unreasonably intrusive.

B. Off-Site Forensic Searches Are "Beyond the Scope" of Routine Border Searches

The *Cotterman* district court's holding comports with Supreme Court jurisprudence in another dimension as well. In a series of search and seizure cases involving exceptions to the warrant or probable cause requirements, the Court has explained that such actions must be limited *in scope* to meet the Fourth Amendment's reasonableness requirement. Searches and seizures that are unreasonable in scope may be subject to more exacting scrutiny.

One of the Court's more illuminating discussions of the Fourth Amendment's reasonable scope requirement appeared in the seminal case *Terry v. Ohio*, which authorized police officers to temporarily stop and frisk—or, seize and search—persons suspected

---

201. Kim, *supra* note 8, at 3, 6; *see also* United States v. Cotterman, 637 F.3d 1068, 1080 (9th Cir. 2011) ("The Court has been careful to distinguish invasive searches of persons from those of a traveler's property, explicitly permitting *highly intrusive searches* of vehicles without suspicion."); Sunil Bector, Note, *"Your Laptop, Please": The Search and Seizure of Electronic Devices at the United States Border*, 24 Berkeley Tech. L.J. 695, 701 (2009).

202. *Flores-Montano*, 541 U.S. at 155; *see also Cotterman,* 637 F.3d at 1085 n.2 (Fletcher, J., dissenting) ("*Flores-Montano* considered whether the disassembly and reassembly of a gas tank was permissible at the border . . . *Flores-Montano* did not address the situation at issue here: whether, without reasonable suspicion, a *total* deprivation of the traveler's possessory interests for an indefinite period is permissible.").

203. *Flores-Montano*, 541 U.S. at 154.

of criminal activity on less than probable cause.[204] The Court found that "in determining whether the seizure and search were 'unreasonable' our inquiry is a dual one—whether the officer's action was justified at its inception, and whether it was *reasonably related in scope* to the circumstances which justified the interference in the first place."[205] In support of this approach, the Court explained that under the Fourth Amendment, the manner in which a seizure and search is conducted is "as vital a part of the inquiry as whether they were warranted at all."[206] Applying this principle to the stop-and-frisk in *Terry*, the Court found that "[a] search for weapons in the absence of probable cause to arrest, however, must, *like any other search*, be strictly circumscribed by the exigencies which justify its initiation."[207] Moreover, the search must be "limited to that which is necessary" to accomplish the precise purpose of the search—in this case, the discovery of weapons.[208]

The Court has continued to impose this reasonable scope requirement in more recent warrantless search cases. In *Horton v. California*, the Court explained that the Fourth Amendment requires "that a warrantless search be circumscribed by the exigencies which justify its initiation."[209] Accordingly, the Court found that "[i]f the scope of the search exceeds that permitted by the terms of a validly issued warrant or the character of the relevant exception from the warrant requirement, the subsequent seizure is unconstitutional without more."[210] Here, the Court described the examples of searches incident to arrest[211] and warrantless vehicle searches[212] that "stray

---

204. Terry v. Ohio, 392 U.S. 1, 27 (1968).

205. *Id.* at 19–20 (emphasis added).

206. *Id.* at 28.

207. *Id.* at 25–26 (emphasis added).

208. *Id.* at 26.

209. Horton v. California, 496 U.S. 128, 129 (1990).

210. *Id.* at 140.

211. *Id.* (citing Coolidge v. New Hampshire, 403 U.S. 443, 517 (1971) (White, J., concurring and dissenting)) (In "a search incident to a lawful arrest, '[i]f the police stray outside the scope of an authorized *Chimel* search they are already in violation of the Fourth Amendment, and evidence so seized will be excluded; adding a second reason for excluding evidence hardly seems worth the candle.'").

212. *Horton*, 496 U.S. at 140–141 (quoting United States v. Ross, 456 U.S. 798, 824 (1982)):

> The scope of a warrantless search of an automobile thus is not defined by the nature of the container in which the contraband is secreted. Rather, it is defined by the object of the search and the places in which there is probable cause to believe that it

outside the scope" of the initial justification for the search, and explained that evidence seized in this manner would be excluded.[213]

In addition, the Supreme Court has elsewhere recognized that a search or seizure "lawful at its inception" may ripen into an illegal search or seizure because of the manner in which it is carried out. In *Place*, the Court held that though the initial seizure and "dog sniff" test of the defendant's luggage were reasonable, the seizure became unreasonable because the length of the ninety-minute detention intruded on the defendant's Fourth Amendment rights.[214] Similarly, in *United States v. Jacobsen*, the Court found that though the initial seizure of a package suspected of containing narcotics was lawful, the officers' destruction of some of the evidence invoked a different balancing of Fourth Amendment interests, "since by destroying a quantity of the powder it converted what had been only a temporary deprivation of possessory interests into a permanent one."[215]

> may be found. . . . Probable cause to believe that a container placed in the trunk of a taxi contains contraband or evidence does not justify a search of the entire cab.

213. *Horton*, 496 U.S. at 140–141. The Court also quoted at length from its decision in *Maryland v. Garrison*, which found that one of the purposes of the Fourth Amendment was to prevent "general searches." *Horton*, 496 U.S. at 139 (quoting Maryland v. Garrison, 480 U.S. 79, 84 (1987)). As the Court reasoned in *Garrison*,

> By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.

Garrison, 480 U.S. at 84. *See also* Arizona v. Hicks, 480 U.S. 321 (1987). In *Hicks*, police officers conducted a warrantless search of the defendant's apartment after receiving a report that a bullet had been shot through the floor and struck another resident. *Id.* at 323. During the course of this search, one of the officers moved some stereo equipment, which he suspected was stolen, in order to see the serial numbers. *Id.* The defendant moved to suppress this latter evidence as the fruit of an unlawful search. *Id.* at 324. The Court found that the officer's moving of equipment was actually a search "separate and apart from" the search that was the lawful objective of the entry into the apartment. *Id.* at 324–25. The Court found that "taking action, unrelated to the objectives of the unauthorized intrusion, which exposed to view concealed portions of the apartment or its contents," actually constituted a "new invasion of respondent's privacy unjustified by the exigent circumstances that validated the entry." *Id.* at 325.

214. United States v. Place, 462 U.S. 696, 709 (1983) ("The length of the detention of respondent's luggage alone precludes the conclusion that the seizure was reasonable in the absence of probable cause.").

215. United States v. Jacobsen, 466 U.S. 109, 124–25 (1984).

Paraphrasing *Place*, the Court explained that "a seizure lawful at its inception can nevertheless violate the Fourth Amendment because its manner of execution unreasonably infringes possessory interests protected by the Fourth Amendment's prohibition on 'unreasonable seizures.'"[216]

As with intrusiveness, the Court has incorporated this principle of limiting searches to a reasonable scope into border search case law. As the Court stated in *Montoya de Hernandez*, the proper inquiry in border search cases involves a balancing between the "sovereign's interests at the border" and the "Fourth Amendment rights" of the individual.[217] In support of its ruling for the government, the Court explained that not only is the individual's expectation of privacy lower at the border, but 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."[218]

This background helps to explain the precise holding in *Montoya de Hernandez*, "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."[219] By using the term "justified at its inception," the holding suggests that a search or seizure that is initially reasonable under the Fourth Amendment, but that goes beyond a reasonable scope, may require a higher level of suspicion—specifically, a "particularized and objective basis for suspecting the particular person" of criminal activity.[220]

This principle also comports with the *Cotterman* district court's decision. In support of its holding, the court explained that a search removed in time and place from the border "represents a

---

216. *Id.* at 124.

217. United States v. Montoya de Hernandez, 473 U.S. 531, 539 (1985).

218. *Id.* at 539–40.

219. *Id.* at 541 (emphasis added).

220. *Id.* at 541–42. Similarly, in *Flores-Montano*, the Court suggested that a longer search that interfered more strongly with the defendant's possessory interests might have been unreasonable. United States v. Flores-Montano, 541 U.S. 149, 155 (2004); *see also* United States v. Laich, No. 08-20089, 2010 WL 259041, at *4 n.8 (E.D. Mich. Jan. 20, 2010) ("[A]ny investigative detention must be properly limited in scope, and the decision to permanently seize Laich's computer, without more, exceeded the permissible limits of the original detention.").

greater intrusion on the person" and requires a higher level of suspicion of criminal activity.[221] In other words, though the initial seizure and search of Cotterman's laptop would have been valid had it occurred at the border, the search *became invalid* when the agents transported the laptop to a different facility. The court was expressly concerned with the government's claimed authority to take possession of the laptop and "move it far away from the border and hold the property for days, weeks or months without any heightened scrutiny."[222] As the court concluded, the government should be required to demonstrate reasonable suspicion of criminal activity "before taking the defendant's computers away from the port of entry."[223]

Thus, like *Place* and *Jacobsen*, *Cotterman* also involved a fact pattern in which the initial search or seizure was permissible, but the government's subsequent actions—transporting the laptop to an off-site facility for a forensic search—transgressed the Fourth Amendment. Following the Supreme Court's examples in *Flores-Montano* and *Montoya de Hernandez*, the *Cotterman* district court also found that searches that are lawful at their inception, but that go beyond the scope of reasonableness, may require heightened suspicion.[224]

---

221. United States v. Cotterman, No. CR 07-1207-TUC-RCC, 2009 WL 465028, at *5 (D. Ariz. Feb. 24, 2009), *rev'd* 637 F.3d 1068 (9th Cir. 2011).

222. *Id.* at *4.

223. *Id.* at *9; *see also* United States v. Alfonso, 759 F.2d 728, 734 (9th Cir. 1985) ("[W]e shall, because of the time factor—the lapse of thirty-six hours in conducting the searches—examine the facts under the rules of extended border search.").

224. *See also* 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, 995–96 (2007) ("[I]mplicit in [the Court's] border search jurisprudence is an indication that some searches go too far. When a non-routine search is not preceded by the appropriate level of suspicion, for example, or when the scope of any search is unreasonable, courts should strike down those inspections as unconstitutional."). The Ninth Circuit Court of Appeals also addressed the "scope" of the laptop search in its *Cotterman* decision. The majority concluded that the 48-hour detention of the defendant's computer was "reasonably related in scope to the circumstances that justified the initial detention at the border." United States v. Cotterman, 637 F.3d 1068, 1082–83 (9th Cir. 2011). However, as Judge Fletcher observed in dissent, the majority ignored the more important question of whether the seizure became unreasonable due to the prolonged detention. *See id*. at 1084 (Fletcher, J., dissenting).

V. EXAMINING THE CONSEQUENCES OF REASONABLE SUSPICION

Part V of this Note examines the policy implications of the *Cotterman* district court's holding, requiring reasonable suspicion for forensic laptop searches at off-site locations following seizures at the border. In support of this rule, this Note proposes that requiring individualized suspicion for this sort of laptop border search puts a necessary check on customs officials—who would otherwise have plenary authority to seize, search, and retain copies of any international traveler's hard drive. As such, even a requirement of reasonable suspicion should better protect innocent travelers from intrusive and unreasonable computer searches.[225]

The sections below defend the *Cotterman* district court decision by addressing its most likely policy-based counterarguments. First, I address whether imposing heightened standards on border officials poses a national security risk, especially if this rule is extended to searches of other, potentially more hazardous containers. Second, I consider whether this decision violates the principle of "technological neutrality" by requiring a different level of suspicion only for border searches of computers. Finally, I discuss whether this decision imprudently grants greater constitutional protections to persons least deserving of such rights.

A. Extending Reasonable Suspicion for Border Searches Poses No National Security Risks

The first and most obvious objection to the *Cotterman* district court decision is that it will impose too high a burden on officials charged with preserving our nation's border security, particularly in a post-9/11 world. Such advocates might contend that current DHS policies are working and essential to national security. In testimony submitted to the Senate Judiciary Committee as part of the June 2008 hearing on laptop border searches, Jayson Ahern, Deputy Commissioner for CBP, stated that "[i]n addition to several successes in arresting individuals possessing child pornography, CBP border searches also have been helpful in limiting the movement of terrorists, individuals who support their activities and threats to

225. *See, e.g.*, *Subcommittee Hearing*, *supra* note 57, at 2 (statement of Sen. Russ Feingold) ("Customs agents must have the ability to conduct even highly intrusive searches when there is reason to suspect criminal or terrorist activity, but suspicionless searches of Americans' laptops and similar devices go too far.").

national security."[226] Two months later, Ahern released a statement arguing that "[m]aking full use of our search authorities with respect to items like notebooks and backpacks, while failing to do so with respect to laptops and other devices, would ensure that terrorists and criminals receive less scrutiny at our borders just as their use of technology is becoming more sophisticated."[227]

Such concerns clearly animated the Ninth Circuit's decision in the *Cotterman* appeal. There, the majority claimed that

> categorically requiring the Government to demonstrate a higher level of suspicion before it may transport property to conduct more thorough and efficient searches . . . would only reward those individuals who, either because of the nature of their contraband or the sophistication of their criminal enterprise, hide their contraband more cleverly or would be inclined to seek entry at more vulnerable points less equipped to discover them.[228]

As the majority later mused, "It seems unlikely that every potential terrorist or purveyor of child pornography would label his or her contraband so that its incriminating nature is immediately recognizable, like 'Kiddie Porn' or 'Plot to Destroy America,' and place it in the middle of an unprotected computer desktop."[229]

Yet, while the *Cotterman* district court's holding would have imposed a new restriction on certain border officials, the burden is not so high that it would interfere with these legitimate law enforcement objectives. That decision would have required only that if government agents intend to search laptops, they must demonstrate reasonable suspicion—a "particularized and objective basis" of criminal activity.[230] This is not a high threshold, and one

---

226. *Subcommittee Hearing*, *supra* note 57, at 53–54 (statement of Jayson P. Ahern, Deputy Comm'r, U.S. Customs & Border Protection). Ahern went on to say that "[d]uring border searches of laptops CBP officers have found violent jihadist material, information about cyanide and nuclear material, video clips of Improvised Explosive Devices (IEDs) being exploded, pictures of various high-level Al-Qaida officials and other material associated with people seeking to do harm to the U.S. and its citizens." *Id*.

227. Jayson Ahern, *Answering Questions on Border Laptop Searches*, Dep't of Homeland Sec. Leadership J. (Aug. 5, 2008), http://www.dhs.gov/journal/leadership/2008/08/answering-questions-on-border-laptop.html.

228. *Cotterman*, 637 F.3d at 1078.

229. *Id.* at 1081 n.15.

230. United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985). As Justice Brennan wrote in his dissent:

that the government has had little trouble meeting in previous border search cases.[231] In fact, the reasonable suspicion standard represents a healthy compromise between a higher (probable cause) standard and a suspicionless search,[232] helping to protect civil liberties without putting an unreasonable burden on border officials.

On the other hand, raising the level of suspicion for off-site searches might also incentivize DHS to upgrade its search capabilities at international ports of entry, where officials would still be legally authorized to conduct suspicionless forensic searches. Such improvements might not be as costly as some critics suggest, particularly in light of recent technological advances in computer forensics. For example, Microsoft has released a digital forensic device that plugs into a computer's USB drive, enabling customs officers to conduct on-site computer searches in a matter of minutes.[233] Should the government choose to implement these faster

---

> The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime. . . . When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or government enforcement agent.

Id. at 552 (Brennan, J., dissenting) (quoting Johnson v. United States, 333 U.S. 10, 13–14 (1948)).

231. *See* Yost, *supra* note 103, at 317 (claiming that because of the ease with which the government has demonstrated reasonable suspicion, "it hardly seems burdensome to require customs agents to have at least some minimum articulable level of suspicion" in laptop border searches); *Subcommittee Hearing*, *supra* note 57, at 181–82 (statement of Lee Tien, Senior Staff Attorney, Electronic Frontier Found.) (claiming that a reasonable suspicion standard is "highly unlikely to impede border agents in their effort to prevent contraband from crossing the border, because it is not a high standard," and concluding, "In virtually all laptop border search cases, courts have found reasonable suspicion."); Coletta, *supra* note 224, at 983 ("The threshold for reasonable suspicion at the border is so low, in fact, that the only circumstance that would likely not meet this standard is a complete lack of suspicion, or a random search.").

232. *See, e.g.*, United States v. McGinnis, 247 F. App'x 589, 594 (6th Cir. 2007) (describing extended border searches "not as border searches (in the sense that no suspicion is required) and not as run-of-the-mine searches (in the sense that a warrant and probable cause are required) but as searches that require something in between—reasonable suspicion").

233. *See* Benjamin J. Romano, *Microsoft Device Helps Police Pluck Evidence From Cyberscene of Crime*, Seattle Times, Apr. 29, 2008, at E1;

forensic technologies at the actual border, rather than shipping every seized computer off to an interior search facility for days at a time, the result would be more efficient border security and less invasive searching.

Nonetheless, critics of the *Cotterman* district court may also have concerns about the consequences for other situations involving items seized at the border and searched elsewhere. Consider the example of a seizure at the border of an item suspected of containing radioactive material, or pathogens, or WMD. In such instances, it would seem cost-prohibitive to require every port of entry to be prepared to conduct all searches on its own premises, no matter how capital-intensive.[234] A more efficient plan would permit the government to maintain the infrastructure and personnel for such searches at centralized locations away from the border.

This was a major concern for the Ninth Circuit Court of Appeals majority, who opined that "requiring forensic computer laboratories at all ports of entry throughout the United States" would put an "unreasonable burden on the Government . . ."[235] Indeed, the majority ridiculed the idea of

> requir[ing] the United States to equip every entry point—no matter how desolate or infrequently traveled—with inspectors and sophisticated forensic equipment capable of searching whatever property an individual may wish to bring within our borders or be otherwise precluded from exercising its right to protect our nation absent some heightened suspicion.[236]

Nevertheless, while it is understandable to be apprehensive about tying the hands of the customs officials responsible for keeping hazardous materials out of the country, the *Cotterman* district court's decision should not lead to this sort of slippery slope. Under that holding, if customs officials deem it necessary to transport a computer seized at the border to another location for a forensic search, this

---

Subcommittee Hearing, *supra* note 57 (statement of Lee Tien, Senior Staff Attorney, Electronic Frontier Found.).

234. *See* Oral Arg. at 13:47, United States v. Cotterman, 637 F.3d 1068 (No. 09-10139), *available at* http://www.ca9.uscourts.gov (follow "Audio and Video" hyperlink; then follow "Advanced Search" hyperlink; then search "by Case Name" for "Cotterman") (claiming that the forensic site located in Tucson was the "first practicable point" where the computer could be searched).

235. United States v. Cotterman, 637 F.3d 1068, 1081 (9th Cir. 2011).

236. *Id*. at 1070.

would be lawful under the Fourth Amendment *so long as* the officials reasonably suspect criminal activity. Thus, the decision would not prohibit agents from conducting exhaustive searches at the actual border, nor would it prevent agents from conducting off-site searches *if* supported by reasonable suspicion.

Applying these principles to container searches involving possible pathogens, WMD, or other hazardous materials, it is clear that a reasonable suspicion requirement would have little effect. First, under that rule, customs officials would only need individualized suspicion that a container held WMD in order to transport it elsewhere for a more extensive search. Second, unlike for computers, border officials should be able to establish the requisite suspicion for containers holding hazardous materials through the use of ordinary security devices—for instance, an x-ray or other scanning technology. In other words, even a normal security scan would reveal enough physical evidence to support an individualized suspicion of hazardous materials. By contrast, with computers, the nature of the container is unique in that often a full forensic scan is required to retrieve any evidence of criminal activity. Therefore, a reasonable suspicion requirement has more impact for these searches, and deliberately so.

In fact, the rationale behind this requirement probably does not reach very far beyond laptops, cell phones, or other electronic data devices. Because of the unique nature of such technology, it is not so difficult to imagine a cursory search returning no evidence of contraband, while a comprehensive forensic search of the same computer might return even incriminating evidence that the owner deleted long ago. As Professor Sara Smyth helpfully describes, it is a "*sui generis* feature of electronic storage devices . . . that they contain vast amounts of information that cannot easily be separated."[237] Thus, because a search of such digital information will necessarily involve processes unique to this technology, it makes it difficult to analogize the *Cotterman* district court's reasoning to other searches, or to extend its rationale to other technologies.

---

237. *See* Smyth, *supra* note 40, at 100. Smyth goes on to claim that this fact "suggests that reading through the enormous volume of information stored on a computer laptop, or some other electronic storage device, gives rise to a much greater infringement of privacy than the examination of a closed container, such as a suitcase or wallet . . . ." *Id.*

B. The Standard for Suspicion Does Not Vary with the Medium, But with the Intrusion

The *Cotterman* district court may invite a separate criticism from those who claim that the level of suspicion required for government searches should not vary with the medium being searched. According to the principle of "technological neutrality," "the overall amount and function of Fourth Amendment protection will be roughly the same regardless of whether a wrongdoer commits his crime entirely online, entirely in the physical world, or using a mix of the two."[238] On this point, Professor Sales claims that the "privacy protections travelers enjoy should not depend on whether they store their data in digital format or on paper."[239] As he argues, "It is hard to see why data stored electronically should be afforded stronger privacy protections than the same data would be if it were stored physically."[240]

The bulk of Sales's argument is against creating a "special exception" that would require reasonable suspicion only for computer searches. Sales suggests that such a rule contradicts the Supreme Court's reasoning in *Ramsey*, which upheld the authority of customs officials to open inbound international mail.[241] There, the Court concluded that "no different constitutional standard should apply simply because the envelopes were mailed, not carried. The critical fact is that the envelopes cross the border and enter this country, not that they are brought in by one mode of transportation rather than another."[242]

Yet, the argument for technological neutrality may be more relevant as a defense of *Arnold* than a critique of *Cotterman*. In fact, the rationale for heightened suspicion does not rest on a special exception for laptop computers. Rather, the reason the district court required heightened suspicion was the manner of the search, which took place 170 miles away from the site of the initial border seizure. As the district court described, such a search "removed in time and place from the border . . . represents a greater intrusion on the person

---

238. Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1015–16 (2010).

239. Sales, *supra* note 40, at 1093.

240. *Id*. at 1115.

241. *Id*. at 1115–17.

242. *Id*. at 1116.

requiring that under the totality of the circumstances, customs officers had reasonable suspicion of criminal activity . . . ."[243]

To put it differently, under the *Cotterman* district court's reasoning, the level of suspicion required for a border search should not vary with the medium. Rather, it should vary with the manner of the search, which the Supreme Court has said must be reasonable in scope and not unduly intrusive.[244] In this way, the lower court's holding does not conflict with the technological neutrality principle. There is no special exception implicated here.

C. The Benefits of Heightened Suspicion Extend to All International Travelers

A final point bears mentioning. It cannot be ignored that *Cotterman* and all of the cases constituting its progeny involve defendants charged with child pornography crimes.[245] As such, the debate over the proper level of suspicion for laptop border searches inevitably raises concerns about regulating the importation of such illicit material into the country.[246]

Nevertheless, the implications of these holdings extend well beyond this isolated group of defendants. The popular outcry in Congress, the national media, and legal circles in response to *Arnold* and more recent CBP and ICE directives shows clearly that these policies have pernicious effects for all sorts of American citizens.[247] Attorneys and other professionals may have privileged or other confidential information searched, copied, and retained by the government indefinitely.[248] International students traveling home

---

243. United States v. Cotterman, No. CR 07-1207-TUC-RCC, 2009 WL 465028, at *5 (D. Ariz. Feb. 24, 2009), *rev'd* 637 F.3d 1068 (9th Cir. 2011).

244. *See supra* Part IV.B.

245. *See supra* Part III.A–B.

246. Congress has been involved with regulating the introduction of digital child pornography into the country since at least 1998. *See* Protection of Children From Sexual Predators Act of 1998, Pub. L. No. 105-314, 112 Stat. 2974 (1998). Current federal law punishes the possession, distribution, and receipt of child pornography with a five- to twenty-year sentence. *See* 18 U.S.C. § 2252 (2006). Importation of child pornography carries the same sentence. *See* 18 U.S.C. § 2260 (2006).

247. *See, e.g.*, Harvey Rishikof, *Combating Terrorism in the Digital Age: A Clash of Doctrines*, 78 Miss. L.J. 381, 383 (2008) (claiming that modern national security threats have made "'border security' and our understanding of the Fourth Amendment, an intellectual pivot point for our expectation of privacy in the 21st century.").

248. *See* Brodsky et al., *supra* note 85.

during semester breaks may experience enormous interferences with deadlines and exam preparation due to suspicionless seizures of their computers.[249] Other law-abiding citizens may suffer extremely intrusive general searches of their most private emails, photographs, financial data, and other effects that the Fourth Amendment is supposed to proscribe.[250]

Thus, while we obviously do not want to adjust border search policy in a way that facilitates the importation of contraband, the full implications of these rules are much broader, reaching all of the more than five hundred million people who cross our border each year, many of them carrying a laptop or other electronic device.[251] As such, though the defendants in this particular line of cases are unsympathetic, civil liberties advocates should remain vigilant that the bad facts in these cases do not lead to bad laws for us all.[252]

VI. CONCLUSION

Though the border search is among the oldest exceptions to the Fourth Amendment's warrant and probable cause requirements, its meaning in modern times remains highly contested. Courts have struggled in recent years in deciding how traditional Fourth

---

249. *See* Press Release, Am. Civil Liberties Union, *supra* note 12; Compl. at 12, *Abidor*, No. CV 10-4059 (E.D.N.Y. filed Sep. 7, 2010).

250. *See Subcommittee Hearing*, *supra* note 57 (statement of Peter Swire, C. William O'Neill Professor of Law, Moritz Coll. of Law, The Ohio State Univ.) ("The text of the Fourth Amendment protects 'persons, houses, papers, and effects.' This constitutional text highlights the framers' deep concerns about personal papers and related documents. There is a long history in the Supreme Court of granting especially strong protection to diaries and similarly personal papers.").

251. Smyth, *supra* note 40, at 84.

252. As Justice Brennan reminds us:

> "[I]t is a fair summary of history to say that the safeguards of liberty have frequently been forged in controversies involving not very nice people." *United States v. Rabinowitz,* 339 U.S. 56, 69 (1950) (Frankfurter, J., dissenting). The standards we fashion to govern the ferreting out of the guilty apply equally to the detention of the innocent, and "may be exercised by the most unfit and ruthless officers as well as by the fit and responsible." *Brinegar v. United States,* 338 U.S. 160, 182, 69 S.Ct. 1302, 1313, 93 L.Ed. 1879 (1949) (Jackson, J., dissenting).

United States v. Montoya de Hernandez, 473 U.S. 531, 548–49 (1985) (Brennan, J., dissenting).

Amendment principles should apply to new technologies in the digital age. The issue of laptop border searches is but one example.

As the debate continues as to the proper level of suspicion needed to conduct these searches, federal courts, Congress, and interested observers should reconsider whether the *Cotterman* district court took the right approach to this issue. Indeed, the holding in that case may fall squarely within the Supreme Court's most recent border search cases. Following *Montoya de Hernandez* and *Flores-Montano*, the Court could find that the privacy and dignity interests implicated in off-site forensic searches, if not their extended scope, demand stronger Fourth Amendment protection.[253]

But *Cotterman*'s importance reaches beyond its precedential value in the laptop border search common law. Perhaps buoyed by *Arnold* and similar decisions by other Courts of Appeals, the executive branch has officially adopted a suspicionless standard for laptop border searches by its agents. Since these policies were implemented, customs officials have begun to push the boundaries of their authority even further, searching computers without suspicion not only at the border, but also at sites within the country's interior.

The *Cotterman* district court rightly rejected the government's argument that the same suspicionless standard should apply to all laptop border searches, regardless of how they are conducted. As such, despite *Cotterman*'s reversal, the decision is nonetheless valuable in proposing an initial, important limitation on the government's subtly expanding border search authority.

---

253. As Justice Jackson has written:

> These [Fourth Amendment rights], I protest, are not mere second-class rights but belong in the catalog of indispensable freedoms. Among deprivations of rights, none is so effective in cowing a population, crushing the spirit of the individual and putting terror in every heart. Uncontrolled search and seizure is one of the first and most effective weapons in the arsenal of every arbitrary government.

Brinegar v. United States, 338 U.S. 160, 180 (1949) (Jackson, J., dissenting).