4-1-2011

Laptops And The Border Search Exception To The Fourth Amendment: Protecting The United States Borders From Bombs, Drugs, And The Pictures From Your Vacation

Victoria Wilson

NOTES

Laptops and the Border Search Exception to the Fourth Amendment: Protecting the United States Borders From Bombs, Drugs, and the Pictures from Your Vacation

VICTORIA WILSON*

I. INTRODUCTION

The Department of Homeland Security asserts that Federal Customs agents have the uninhibited right to detain international travelers at the border while they search the contents of their laptops, cell phones, and other electronic devices without any individualized suspicion of wrongdoing.[1] In 2008 the Department of Homeland Security first released its policy, which allowed customs agents to search, copy, and retrieve contents of a laptop computer, including confiscating the laptop itself for a reasonable period of time without any individualized suspicion.[2] The policy has alarmed many travelers[3] and prompted the American Civil Liberties Union to file suit on August 26, 2009, seeking records on the Customs and Border Protection's policy of searching travelers' laptops.[4] The very next day, the Department of Homeland Security released a revised policy limiting the amount of time that electronic devices can be held by customs officers. It also states that infor-

* J.D. Candidate 2011, University of Miami School of Law; B.S. 2007, University of Florida. Thank you to Professor Ricardo Bascuas for his guidance throughout the writing process.

1. *See* U.S. Customs and Border Protection, Border Search of Electronic Devices Containing Information, CBP Directive No. 3340-049 § 1 (August 2009).

2. U.S. Customs and Border Protection, *Policy Regarding Border Search of Information* (July 16, 2008), http://www.cbp.gov/linkhandler/cgov/travel/admissibility/search_authority.ctt/search_authority.pdf.

3. Editorial, *Laptop seizures 'truly alarming,'* MARSHFIELD NEWS-HERALD, Aug. 19, 2008, at A6; Thomas Claburn, *DHS Clarifies Laptop Border Searches*, INFORMATIONWEEK GOVERNMENT, Aug. 28, 2009, http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=219500468.

4. Complaint at 3, 6, Am. Civil Liberties Union v. Dep't of Homeland Sec., 2009 WL 2627670 (S.D.N.Y. Aug. 26, 2009) (No. 09 Civ. 7465). The first documents released by Customs and Border Protection revealed that in nine months over 1,500 electronic devices were searched, cell phones being the most common. Other devices searched include digital cameras, thumb drives, DVDs and hard drives. American Civil Liberties Union, *Customs and Border Protection (CBP) First Production Documents* (Jan. 14, 2010), http://www.aclu.org/national-security/customs-and-border-protection-cbp-first-production-documents.

mation from electronic devices can now only be retained if there is probable cause that a crime has been committed;[5] however, a customs officer may still search electronic devices and may review and analyze the information encountered at the border without any suspicion.[6] The Department of Homeland Security claims this policy is justified because the searches of these devices can:

> help detect evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography. They can also reveal information about financial and commercial crimes, such as those relating to copyright, trademark and export control violations. Finally, searches at the border are often integral to a determination of admissibility under the immigration laws.[7]

The Department of Homeland Security has also stated that of the 144 million international travelers between October 1, 2008 and May 5, 2009, only 1947 were subject to searches of their electronic devices.[8] Several courts have upheld the powers asserted in this policy, holding that the search of files contained within electronic storage devices does not require any level of suspicion at the border.[9] In an amicus brief filed on behalf of the defendant-appellee in *United States v. Arnold*, the American Civil Liberties Union pointed out that a single case "offers a rare glimpse inside our border officials' systematic but unchecked policy of randomly searching, seizing, and copying the contents of travelers' laptop computers."[10]

It may seem easier to uphold a policy where the cases before the court concern child pornography, as most of them have, but courts sometimes may not recognize the broader picture of the systematic intrusions inflicted on innocent people.[11] Hundreds of travelers have had to

---

5. *See* U.S. Customs and Border Protection, Border Search of Electronic Devices Containing Information, CBP Directive No. 3340-049 §§ 5.3.1, 5.4.1.1 (August 2009).

6. *See id.*

7. *Id.* § 1.

8. DHS Privacy Office, Annual Report to Congress, July 2008–June 2009 54 (Sept. 2009), httyp://www.dhs.gov/gov/xlibrary/assets/privacy/privacy_rpt_annual_2009.pdf.

9. *See, e.g.*, United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008); United States v. Singh, 295 F. App'x 190, 190 (9th Cir. 2008); United States v. Linarez-Delgado, 259 F. App'x 506, 507–08 (3d Cir. 2007); Singh v. Scott, No. CV 08-86-GF-SHE, 2009 WL 2370636, at *5 (D. Mont. July 29, 2009). United States v. Bunty, No. 07-641, 2008 WL 2371211, at *3 (E.D. Pa. June 10, 2008); United States v. Hampe, No. 07-3-B-W, 2007 WL 1192365, at *4 (D. Me. Apr. 18, 2007).

10. Brief for Association of Corporate Travel Executives and Electronic Frontier Foundation as Amici Curiae Supporting Defendant-Appellee at 14, United States v. Arnold, 533 F.3d 1003 (2008) (No. 05-772), *available at* http://www.eff.org/files/filenode/US_v_arnold/arnold_amicus.pdf.

11. "There may be, and I am convinced that there are, many unlawful searches of . . . innocent people which turn up nothing incriminating, in which no arrest is made, about which

stand by and wait for sometimes hours while strangers rummage through their emails, photos, browser history, and documents.

Although the percentage of travelers who have had their laptops searched at the border seems small, the judicial support of this policy means that investigative resources are currently the only thing limiting the number of electronic devices searched at the border. In *United States v. Ickes*, the court stated that "[c]ustoms agents have neither the time nor the resources to search the contents of every computer."[12] However, advances in technology along with judicial approval will likely result in the increase in searches of electronic devices as customs improve their ability to search.[13] Furthermore, lacking the resources to search on a mass scale is different from having the right to search.

This comment reviews the protections provided by the Fourth Amendment at the border and argues that the border exception to the Fourth Amendment does not justify the suspicionless search of information contained within computer files. Part II examines the history and the modern application of the border exception to the Fourth Amendment. Part III introduces the application of the border exception to electronic storage devices. Part IV argues that the purpose of the border exception does not support the suspicionless searches of information contained within a laptop, and such searches only serve general law enforcement goals; therefore, the search of laptop files falls outside the scope of a reasonable border search. Part V argues the border exception should not apply to a device that can only contain information. First, the government's need to search data and information is lower and the traveler's interest in the free flow of information weighs against that need. Second, the treatment of correspondence contained within international mail underscores the caution courts demonstrate when dealing with the reading of correspondence, and highlights the inconsistencies between the treatment of information in international mail and laptops at the border. Part VI concludes, briefly explaining that the border exception should not apply to the supicionless search of the files within a laptop.

---

courts do nothing, and about which we never hear." Brinegar v. United States, 338 U.S. 160, 181-82 (1949) (Jackson, J., dissenting).

12. 393 F.3d 501, 506–07 (4th Cir. 2005) (stating that the possibility that "any person carrying a laptop computer . . . on an international flight would be subject to a search of the files on the computer 'hard drive'" was "far-fetched").

13. *See Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel: Hearing Before the Subcomm. on the Constitution, Civil Rights and Property Rights of the S. Comm. on the Judiciary*, 110th Cong (2008) (statement of Lee Tien, Senior Staff Attorney, Electronic Frontier Foundation) at 10, *available at* http://www.eff.org/files/filenode/travelscreening/tien%20testimony.pdf (discussing the technological advancements that could be used to increase customs ability to search electronic devices at the border).

II. SEARCHES UNDER THE FOURTH AMENDMENT AND THE BORDER EXCEPTION

There are two theories interpreting what is required by the Fourth Amendment before a governmental search can be conducted; the "warrant preference"[14] theory and the "generalized reasonableness"[15] theory. Under both of these approaches, some level of individualized suspicion is generally required by the Fourth Amendment before the government may conduct a search.[16] There are a few narrowly drawn exceptions to the requirement of individualized suspicion such as searches that serve "special needs, beyond the normal need for law enforcement," sobriety checkpoints, and border searches.[17] Furthermore, whether authorized by warrant, probable cause, or a Fourth Amendment exception, government searches must be justified at inception and reasonably related in scope to circumstances which justified interference in the first place.[18]

A. *Border Searches and the Fourth Amendment*

The routine border search is among the few searches that can be made without any individualized suspicion at all. The Constitution gives

14. Under the "warrant preference" theory, the Fourth Amendment generally requires a warrant or probable cause, *see, e.g.*, Katz v. United States, 389 U.S. 347, 357 (1967), although there are certain exceptions, including the border exceptions. *See generally* United States v. Flores-Montano, 541 U.S. 149 (2004); United States v. Montoya de Hernandez, 473 U.S. 531 (1985); United States v. Ramsey, 431 U.S. 606 (1977). Probable cause exists when there is a fair probability that evidence of a crime will be found in a particular place, *see, e.g.*, United States v. Grubbs, 547 U.S. 90, 95 (2006) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)).

15. Under the "generalized reasonableness" theory, the Fourth Amendment requires searches and seizures to be reasonable and sometimes reasonableness may require a warrant, probable cause, or reasonable suspicion, *see* Ricardo Bascuas, *Fourth Amendment Lessons From the Highway and the Subway: A Principled Approach to Suspicionless Searches*, 38 RUTGERS L.J. 719, 724–25 (2007), depending on a balance of privacy interests and government objectives. *See* Samson v. California, 547 U.S. 843, 864 (2006). Reasonable suspicion is a less demanding standard than probable cause and requires only specific and articulable facts that suggest an individual is engaged in criminal activity. *See, e.g.*, Illinois v. Wardlow, 528 U.S. 119, 123 (2000) (holding that flight from police officers in a high crime area is sufficient to find reasonable suspicion).

16. *See* United States v. Martinez-Fuerte, 428 U.S. 543, 560 (1976) ("[S]ome quantum of individualized suspicion is usually a prerequisite to a constitutional search or seizure.").

17. *See* City of Indianapolis v. Edmond, 531 U.S. 447, 451–52 (2000).

18. *See, e.g.*, Arizona v. Hicks, 480 U.S. 321, 325 (1987) ("Taking action, unrelated to the objectives of the authorized intrusion, which exposed to view concealed portions of the apartment or its contents, did produce a new invasion of privacy, unjustified by the exigent circumstance that validated the entry."); New Jersey v. T.L.O., 469 U.S. 325, 341–42 (1985) (stating that a search of schoolchildren "will be permissible in its scope when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the age and sex of the student and the nature of the infraction"); Chimel v. California, 395 U.S. 752, 762–63 (1969) (search incident to arrest); Terry v. Ohio, 392 U.S. 1, 19 (1968) ("When an officer has probable cause to search a car, she may only search in places where the items in question may reasonably be located including any container in the vehicle.").

Congress broad powers "[t]o regulate Commerce with foreign Nations"[19] and Congress has used this power to give the Executive "plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country."[20] Under the "warrant preference" approach, the border search doctrine is an exception to the warrant and probable cause requirements of the Fourth Amendment.[21] Under the "generalized reasonableness theory," the government's interest in preventing the entry of unwanted persons and items has been said to be "at its zenith" at the international border,[22] and the individual's expectation of privacy lower at the border.[23]

B. *History of the Border Exception*

Searches at the United States border have not been subject to traditional Fourth Amendment protections since the Bill of Rights was created.[24] The justifications for the exception, however, have evolved over time as newly perceived threats at the border have emerged. The same Congress that framed the Fourth Amendment also passed a statute allowing for warrantless searches at the border for the regulation of import duties.[25] One hundred years later, in *United States v. Boyd*, the Court still focused on the government's financial interest in taxing imports.[26] However, forty years after *Boyd*, when there was a concern over importation of contraband during prohibition,[27] the Court adopted a national security justification for the exception. The Court concluded that "national self protection" made it reasonable for border agents to search vehicles to determine if the individuals were entitled to enter the country and if their effects could be lawfully brought in.[28]

The Supreme Court did not explicitly allow routine suspicionless

---

19. U.S. CONST. art. I, § 8, cl. 3.

20. United States v. Flores-Montano, 541 U.S. 149, 153 (2004) (quoting United States v. Montoya de Hernandez, 453 U.S. 531, 537 (1985)).

21. *See* California v. Acevedo, 500 U.S. 565, 582 (1991) (Scalia, J., concurring) (quoting Craig M. Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1473–74 (1985)).

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

23. *Montoya de Hernandez*, 473 U.S. at 539.

24. *See* Act of July 31, 1789, ch. 5 §§ 23–24, 1 Stat. 29, 43; Untied States v. Ramsey, 431 U.S. 606, 616 (1977).

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

26. *See* 116 U.S. 616, 634 (1886).

27. *See* Robert Post, *Federalism, Positive Law, and the Emergence of the American Administrative State: Prohibition in the Taft Court Era*, 48 WM. & MARY L. REV. 1, 118–22 (2006).

28. *See* Carroll v. United States, 267 U.S. 132, 154 (1925).

searches until 1985 in *United States v. Montoya de Hernandez*,[29] during a substantial escalation of the "war on drugs."[30] The Court relied on *Ramsey* and *United States v. Carroll* to show that routine suspicionless searches were well established,[31] although "neither of those decisions went that far."[32] In *United States v. Ramsey*, the Court concluded that probable cause was not required to open international mail suspected of containing drugs based on "the recognized right of the sovereign to control . . . who and what may enter the country."[33] Courts continue to rely on the long history of the border exception to support the idea that modern suspicionless border searches are firmly established in history.[34] This reliance is misplaced because modern border searches have evolved substantially from the first border statute. The statute passed by the First Congress reflected a financial interest in searching at the border,[35] while the power to search at the border is now considered necessary to prevent smuggling and to prevent prohibited and dangerous items from entering the United States.[36] The officials only had the power to search when there was "reason to suspect any goods, wares or merchandise subject to duty shall be concealed."[37] Some of the modern statutes authorizing customs officers to search at the border now omit the "reason to suspect" language,[38] which courts have interpreted to allow customs officials to conduct routine searches without any suspicion at all.[39] Although the

29. 473 U.S. 531, 538 (1985); Christopher Lee, Comment, *The Viability of Area Warrants in a Suspicionless Search Regime*, 11 U. PA. J. CONST. L. 1015, 1025 (2009).

30. *See* United States v. Montoya de Hernandez, 573 U.S. 531, 538–39 (1985) (stating that concern for the protection of the border is "heightened by the veritable national crisis in law enforcement caused by smuggling of illicit narcotics"); Diane Michele Krasnow, *To Stop the Scourge: The Supreme Court's Approach to the War on Drugs*, 19 AM. J. CRIM. L. 219, 226 (1992).

31. *See Montoya de Hernandez*, 431 U.S. at 538 n.1.

32. Lee, *supra* note 29, at 1024; *see also* United States v. Ramsey, 431 U.S. 606, 615 n.10 (1977) (finding it unnecessary to decide the level of suspicion required under other statutory authority because customs officials had reasonable cause to suspect a violation of customs laws, as required by 19 U.S.C. § 482); *Carroll*, 267 U.S. at 154.

33. *See Ramsey*, 431 U.S. at 619–21.

34. *See, e.g.*, United States v. Arnold, 533 F.3d 1003, 1007 (9th Cir. 2008) ("Courts have long held that searches of closed containers and their contents can be conducted at the border without particularized suspicion under the Fourth Amendment."); Rahman v. Chertoff, 530 F.3d 622, 624 (7th Cir. 2008) ("The modern statute . . . derived from a statute passed by the First Congress . . . and reflects the 'impressive historical pedigree' of the Government's power and interest." (quoting United States v. Villamonte-Marquez, 462 U.S. 579, 584 (1983))); United States v. Whitted, 541 F.3d 480, 484 (3d Cir. 2008); United States v. Ickes, 393 F.3d 501, 505 (4th Cir. 2005) (quoting *Ramsey*, 431 U.S. at 619).

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

36. *See, e.g.*, *Ramsey*, 431 U.S. at 618–19 (quoting United States v. 12 200-Ft. Reels of Film, 413 U.S. 123, 125 (1973)).

37. Act of July 31, 1789, ch. 5, § 24, 1 Stat. 29, 43.

38. *See, e.g.*, 19 U.S.C. § 1581(a) (2000).

39. *See, e.g.*, United States v. Flores-Montano, 541 U.S. 149, 155 (2004); United States v.

border exception has a long history, the explicit recognition of suspicionless searches at the border is fairly new, and the original justification for border searches has expanded substantially since the first border statute.

C. *Modern Border Searches and Reasonableness*

Although border searches are exempt from the Fourth Amendment warrant requirement, they are still subject to the reasonableness requirement.[40] Courts have found that reasonableness only requires officials to have some level of suspicion when the search is either nonroutine, or destructive.[41]

In *United States v. Montoya de Hernandez*, the Court first articulated two different levels of searches at the border; routine searches and nonroutine searches.[42] Routine searches at the border do not require reasonable suspicion, probable cause, or a warrant, while nonroutine searches do require reasonable suspicion.[43] The distinction turns on the extent to which the search is an invasion of privacy, as balanced against the government's interest to search at the border.[44] Pat-downs, frisks, luggage searches, and automobile searches are all considered routine searches that do not require any level of individualized suspicion.[45] According to several courts, this category also includes searches of the files on laptops and other electronic storage devices.[46]

Nonroutine searches involve a high degree of intrusion and often involve the exposure of intimate body parts.[47] The Supreme Court identified body cavity, x-ray, and strip searches as nonroutine.[48] Courts have

---

Montoya de Hernandez, 473 U.S. 531, 538 (1985); United States v. Ickes, 393 F.3d 501, 504 (4th Cir. 2005).

40. *See, e.g.*, *Montoya de Hernandez*, 473 U.S. at 537–38; United States v. Hyde, 37 F.3d 116, 119–20 (3d Cir. 1994).

41. *See Flores-Montano*, 541 U.S. at 152, 155–56.

42. *See Montoya de Hernandez*, 473 U.S. at 538, 541.

43. *See, e.g.*, *id.* at 538; United States v. Ramsey, 431 U.S. 606, 616–19 (1977); Almeida-Sanchez v. United States, 413 U.S. 266, 272–73 (1973).

44. *See Flores-Montano*, 541 U.S. at 152.

45. *See* Denson v. United States, 574 F.3d 1318, 1340 (11th Cir. 2009); United States v. Whitted, 541 F.3d 480, 485 (3d Cir. 2008); United States v. Irving, 352 F.3d 110, 124–25 (2d Cir. 2006).

46. *See* United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008); United States v. Singh, 295 F. App'x 190, 190 (9th Cir. 2008); United States v. Linarez-Delgado, 259 F. App'x 506, 507–08 (3d Cir. 2007); Singh v. Scott, No. CV 08-86-GF-SHE, 2009 WL 2370636, at *5 (D. Mont. July 29, 2009). United States v. Bunty, No. 07-641, 2008 WL 2371211, at *3 (E.D. Pa. June 10, 2008); United States v. Hampe, No. 07-3-B-W, 2007 WL 1192365, at *4 (D. Me. Apr. 18, 2007).

47. *See Flores-Montano*, 541 U.S. at 152; United States v. Barrow, 448 F.3d 37, 41 (1st Cir. 2006); United States v. Tsai, 282 F.3d 690, 694 (9th Cir. 2002).

48. *See* United States v. Montoya de Hernandez, 437 U.S. 531, 537 (1985).

drawn distinctions between total strip searches and other searches that only necessitate exposure of body parts commonly shown in public.[49]

However, in *United States v. Flores-Montano*, the Court limited the classification of searches as nonroutine, stating that "[c]omplex balancing tests to determine what is a 'routine' vehicle search, as opposed to a more 'intrusive' search of a person, have no place in border searches of vehicles."[50] Several courts have interpreted *Flores-Montano* to hold that the routine and nonroutine distinction is inapplicable to searches of property; therefore, the only time the search of property requires reasonable suspicion is when the search is destructive.[51]

This is not a necessary result of *Flores-Montano* because the holding was limited to vehicles. One court after *Flores-Montano* classified the search of a passenger cabin of a ship as nonroutine because it is more like a home, expanding the category of nonroutine beyond physical bodily intrusion.[52] In that case, the court distinguished the facts from *Flores-Montano*, stating "[w]hereas the 'dignity and privacy interests of the person' do not carry over to border searches of an automobile, the privacy interests of an individual in his or her living quarters are significantly greater and compel more rigorous Fourth Amendment protection."[53] This case illustrates that *Flores-Montano* did not completely preclude the possibility that the search of property can be intrusive enough as to be considered nonroutine. The distinction between bodily searches and the search of property at the border has important implications when applied to laptops because there would be nothing limiting the reasonable scope of a laptop search, so long as the search isn't destructive. Although the possibility of classifying property as nonroutine may have been left open by the Court, lower courts have generally rejected arguments that laptops should be classified as such.[54]

III. APPLICATION OF THE REASONABLENESS REQUIREMENT TO THE CONTENTS OF LAPTOPS

For searches of files stored on a laptop, courts have found the reasonableness requirements is met "simply by virtue of the fact that they

49. *See, e.g.*, United States v. Ramos-Saenz, 36 F.3d 59, 61 (9th Cir. 1994) (removing shoes does not reach the degree of intrusiveness present in strip and body cavity searches); United States v. Charleus, 871 F.2d 265, 268 (2d Cir. 1989) (lifting up a man's shirt considered routine).

50. 541 U.S. at 152.

51. *See* United States v. Arnold, 533 F.3d 1003, 1007 (9th Cir. 2008); United States v. Romm, 455 F.3d 990, 997 n.11 (9th Cir. 2006); United States v. Flores-Montano, 424 F.3d 1044, 1049 n. 6 (9th Cir. 2005).

52. *See* United States v. Whitted, 541 F.3d 480, 488 (3d Cir. 2008).

53. *Whitted*, 541 F.3d at 488.

54. *See*, e.g., *Arnold*, 533 F.3d at 1008; United States v. Singh, 295 F. App'x 190, 190 (9th Cir. 2008).

occur at the border,"[55] regardless whether there is any individualized suspicion and without any limitations in scope. Applying the privacy balancing test, courts have only found two categories of searches where the privacy invasion is high enough to require individualized suspicion at the border—bodily intrusions, and intrusions into areas that are like a home.[56] Therefore, everything else at the border, such as luggage, requires no individualized suspicion. As a result, border search cases have turned on the strength of dueling analogies.

Several defendants have argued that the search of data contained within a laptop at the border should require some level of individualized suspicion because they are extremely private. But courts have generally rejected these arguments and held that the search of electronic storage devices at the United States border is routine and does not require any level of individualized suspicion.[57]

On July 17, 2005, Michael Arnold landed at Los Angeles International Airport.[58] Customs officials were inspecting his luggage when they came across a laptop, and they asked Arnold to boot it up.[59] The desktop displayed several icons and folders, two of which were entitled "Kodak photos" and "Kodak memories."[60] The officers clicked on those folders and examined the photos on Arnold's laptop, one of which depicted two nude women.[61] He was then questioned and detained by special agents for several hours while the files on his computer were further inspected.[62] Several pictures depicting child pornography were found on his computer.[63] The district court granted Arnold's motion to suppress the photos because the government conducted the search without reasonable suspicion.[64] The Ninth Circuit reversed, holding that "reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage device at the border."[65] In

55. *See, e.g., Arnold* 533 F.3d at 1006.

56. *See, e.g.*, United States v. Montoya de Hernandez, 437 U.S. 531, 537 (1985); United States v. Whitted, 541 F.3d 480, 485 (3d Cir. 2008).

57. *See Arnold*, 533 F.3d at 1008; United States v. Singh, 295 F. App'x 190, 190 (9th Cir. 2008); United States v. Linarez-Delgado, 259 F. App'x 506, 507–08 (3d Cir. 2007); Singh v. Scott, No. CV 08-86-GF-SHE, 2009 WL 2370636, at *5 (D. Mont. July 29, 2009). United States v. Bunty, No. 07-641, 2008 WL 2371211, at *3 (E.D. Pa. June 10, 2008); United States v. Hampe, No. 07-3-B-W, 2007 WL 1192365, at *4 (D. Me. Apr. 18, 2007).

58. *Arnold*, 533 F.3d at 1005.

59. *Id.*

60. *Id.*

61. *Id.*

62. *Id.*

63. *Id.*

64. United States v. Arnold, 454 F. Supp. 2d 999, 1007 (C.D. Cal. 2006) (overruled by United States v. Arnold, 533 F.3d 1003 (9th Cir. 2008)).

65. *Arnold*, 533 F.3d at 1008.

Arnold, the court reasoned that the search of a laptop or other electronic device is not logically any different from the search of a traveler's luggage, rejecting the defendant's argument that the search of a laptop is more like the search of a home based on a laptop's storage capacity.[66]

Another district court rejected the argument that the search of a computer is analogous to a bodily search in *United States v. McAuley*.[67] A defendant even argued, in *United States v. Cotterman*, that searching a laptop is the equivalent of a body cavity search because a laptop "is likely to hold an individual's most private thoughts and information."[68] The court found that it was "not a case of a body cavity search where reasonable suspicion would be required because of the personal intrusiveness of the search,"[69] but instead found reasonable suspicion was required because it was an "extended border search,"[70] which occurred 170 miles from the border and took thirty six hours.[71] The privacy focus has also spawned extensive arguments describing the vast amount of storage capacity computers have[72] and the types of information they may contain,[73] in order to make them comparable to the human mind or an extension of the person.[74]

These cases reflect a problem with the balancing test at the border

66. *See Arnold*, 533 F.3d at 1009 (9th Cir. 2008).

67. *See* 563 F. Supp. 2d 672, 677 (W.D. Tex. 2008).

68. No. CR 07-1207-TUC-RCC, 2009 WL 465028, at *3 (D. Ariz. Feb. 24, 2009).

69. *Id.* at *4.

70. Extended border searches occur when a search is removed in time and place from the border and must be justified by reasonable suspicion. *Id.* at *5.

71. *See id.* at *9.

72. *See, e.g.*, Brief for Association of Corporate Travel Executives and Electronic Frontier Foundation as Amici Curiae Supporting Defendant-Appellee at 14, United States v. Arnold, 533 F.3d 1003 (2008) (No. 05-772) ("The volume of information stored on computers means that the privacy invasion of a laptop border search is enormous."); Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 569 (2005); Sarah M. Smith, Comment, *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, 71 (2009) (protection of personal information is critical due to the "ability of electronic devices to store vast amounts of . . . information").

73. *See, e.g.*, Brief for Defendant-Appellant at 13, United States v. Singh, No. 07-30421 13 (9th Cir. 2008); Ordean L. Volker, *Lawyers, Laptops, and the Border*, 72 TEX. B. J. 640, 641 (2009); Erick Lucadamo, Note, *Reading Your Mind at the Border: Searching Memorialized Thoughts and Memories on Your Laptop and* United States v. Arnold, 54 VILL. L. REV. 541, 574 (2009) (listing privileged information and trade secrets); Kindal Wright, Comment, *Border Searches in a Modern World: Are Laptops Merely Closed Containers, or are They Something More?*, 74 J. AIR L. & COM. 701, 721 (2009) ("precious memories").

74. *See, e.g.*, United States v. Arnold, 454 F. Supp. 2d 999, 1000 (overruled by United States v. Arnold, 533 F.3d 1003 (9th Cir. 2008)) (finding that Fourth Amendment protection extends to the search of this type of personal and private information at the border, because "electronic storage devices function as an extension of our own memory"); Brief for Defendant-Appellant at 13, United States v. Singh, No. 07-30421 13 (9th Cir. 2008) ("What the government ignores is how a search of a laptop is really the equivalent of a search of someone's personal thoughts.").

because they don't comply with the public's expectations and because they are not supported by the purpose of the border exception as discussed in Part IV. A computer probably doesn't stand much of a chance at being more like a person's cavity than a briefcase; however, there is still something different about searching a laptop, as opposed to luggage, that makes people generally uncomfortable.[75] It shows that there is a strong privacy interest in the contents of a laptop. But people aren't surprised when their physical papers, diaries and photo albums can be searched at the border. So, why are people so surprised when they learn that their laptops can be searched without suspicion? It might be the amount of information a laptop can contain, but it is likely something more than that. It shows that generally travelers don't expect that the government can do that, despite all the searches that are regularly conducted at the border. People don't expect that their laptops can be searched because it seems on an intuitive level that something about it doesn't make sense. People accept that their personal items need to be searched at the border in order to regulate importation of contraband and dangerous items. The surprise, therefore, may reflect an understanding that the search of electronic files is not supported by the justification for the border exception in the first place; they aren't going to find bombs, drugs, or disease wielding fruits within a computer.

IV. THE PURPOSE OF THE BORDER EXCEPTION

The purpose of exempting searches at the border from traditional Fourth Amendment protections does not justify electronic informational searches without suspicion. The purpose of the border exception is to regulate who and what may enter the country in order to intercept prohibited or dutiable items and things that would be dangerous to the country such as bombs, weapons, communicable diseases, narcotics, or explosives.[76] However, courts do not consider this rationale when evaluating the reasonableness of border searches. As discussed above, the only limitations to the scope of a suspicionless border search turns on intrusiveness, or whether a search is destructive.[77] The application of the reasonableness requirement is also limited by the Supreme Court's cir-

75. *See supra* note 3.

76. United States v. Montoya de Hernandez, 453 U.S. 531, 544 (1985); United States v. Villamonte-Marquez, 462 U.S. 579, 591 (1983); United States v. 12 200-Ft. Reels of Film, 413 U.S. 123, 125 (1973); Carroll v. United States, 267 U.S. 132, 154 (1925); United States v. Guzman-Padilla, 573 F.3d 865, 886 (9th Cir. 2009); United States v. Alfonso, 759 F.2d 728, 733 (1985) (citing 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.").

77. United States v. Seljan, 547 F.3d 993, 1000 (9th Cir. 2008) (quoting United States v. Ramsey, 431 U.S. 606, 618 n.13 (1977)).

cular reasoning that although the reasonableness requirement applies at the border, routine border searches are reasonable by virtue of the fact they occur at the border.[78]

A. *Proposed Analysis of Border Searches*

Like other searches under the Fourth Amendment, the reasonableness of searches at the border should also depend on the scope of the intrusion, the manner of its conduct, and the justification for its initiation.[79] Under the current analysis, the manner of the search only matters if the search of property is destructive, and the scope is only limited by whether the intrusion is comparable to a cavity search or the search of a home. It does not matter whether the initial search is justified by to the need to intercept dangerous item, or whether the scope is limited to enforcing customs laws. The purpose of the border exception should play a larger role in the classification of a border search as nonroutine. This analysis would allow for the protection of privacy that courts are concerned with in regards to cavity searches, as well as limit the scope of a routine search to the purpose and rationale for exempting searches at the border in the first place.

1. The Rationale of the Border Exception Does not Justify Initiating a Search of Electronic Files

A search at the border that does not rationally fit within the purpose of the border exception should be considered nonroutine. The justification of the border exception has expanded over time, reflecting the changing concerns at the border, such as importation of alcohol during the prohibition and the rise of international narcotics trafficking.[80] Modern courts have described the border exception as being necessary to intercepting prohibited or dutiable items and things that would be dangerous to the country such as bombs, weapons, communicable diseases, narcotics, or explosives.[81] Put more simply, the purpose is to regulate

78. *See Ramsey*, 431 U.S. at 616.

79. *See* United States v. Duncan, 693 F.2d 971, 977 (9th Cir. 1982).

80. The national security justification for the border exception was first adopted when there was a concern about illegal importation of alcohol during prohibition. *See* Carroll v. United States, 267 U.S. 132, 154 (1925); Robert Post, *Federalism, Positive Law, and the Emergence of the American Administrative State: Prohibition in the Taft Court Era*, 48 Wm. & Mary L. Rev. 1, 118–22 (2006). The Supreme Court first explicitly recognized routine suspicionless border searches in 1985 during a substantial escalation of the "war on drugs." *See* United States v. Montoya de Hernandez, 573 U.S. 531, 538–39 (1985) (stating that concern for the protection of the border is "heightened by the veritable national crisis in law enforcement caused by smuggling of illicit narcotics"); Diane Michele Krasnow, *To Stop the Scourge: The Supreme Court's Approach to the War on Drugs*, 19 Am. J. Crim. L. 219, 226 (1992).

81. United States v. Montoya de Hernandez, 453 U.S. 531, 544 (1985); United States v.

who and what may enter the country. In addition to the collection of tax on dutiable items, the ability to search at the border is necessary to regulate the importation of dangerous items and prevent the spread of disease that can be contained in things like fruits and vegetables. Border searches should be treated uniquely for these purposes, but once the search extends well beyond the logical purpose, the search should be subject to some level of suspicion. In a concurring opinion, Judge Berzon recognized that:

> a search which happens to be at the border but is not motivated by either of these two "national self protection" interests [regulating who and what may enter the country] may not be "routine" in the sense that term is used in the border search cases, as it is not within the rationale for declaring such searches reasonable without a warrant or probable cause.[82]

The emphasis on privacy in the context of border searches often eliminates a discussion of the purpose behind the border exception in determining the scope of a routine search.[83] The cases start from the premise that everything can be searched at the border unless it is private or the search is destructive. The reasonableness of laptop searches at the border should be based upon whether the purpose and the rationale behind the border exception justify the search of a device that can only contain data. Because the distinction between routine and nonroutine searches at the border has centered on degrees of privacy intrusion, arguments regarding what level of suspicion should be required for a particular search depend on strained analogies to things the court has considered sufficiently private at the border. Several courts have found that the suspicionless search of a passenger cabin of a ship is nonroutine because it is more like a home,[84] which reflects the high regard courts have for the privacy of the home in ordinary Fourth Amendment jurisprudence. In *United States v. Sanders*, the defendant argued that a search

---

Villamonte-Marquez, 462 U.S. 579, 591 (1983); United States v. 12 200-Ft. Reels of Film, 413 U.S. 123, 125 (1973); Carroll v. United States, 267 U.S. 132, 154 (1925); United States v. Guzman-Padilla, 573 F.3d 865, 886 (9th Cir. 2009); United States v. Alfonso, 759 F.2d 728, 733 (1985) (citing 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.").

82. United States v. Tsai, 282 F.3d 690, 699 (9th Cir. 2002) (Berzon, J., concurring).

83. *See, e.g.*, United States v. Arnold, 533 F.3d 1003, 1007 (9th Cir. 2008) (briefly mentioning the justification of the doctrine and focusing on whether the search of a laptop is intrusive or destructive); United States v. Ramos-Saenz, 36 F.3d 59, 61 (9th Cir. 1994) (finding a border search is nonroutine only when it reaches the degree of intrusiveness present in a strip search or body cavity search); United States v. McAuley, 563 F. Supp. 2d 672, 676 (W.D. Tex. 2008) ("The key variable . . . is 'the invasion of the privacy and dignity of the individual.'" (quoting United States v. Sandler, 644 F.2d 1163, 1167 (5th Cir. 1981))).

84. *See* United States v. Whitted, 541 F.3d 480, 488 (3d Cir. 2008); United States v. Cunningham, No. 98-265, 1996 WL 665747, at *3 (E.D. La. 1996).

of an artificial leg was analogous to the search of a body cavity.[85] The fact that many people are alarmed that the government can search computer files at the border reflects how the courts understanding of privacy and the government's needs at the border do not converge with what the public understands the purpose of border searches to be. Instead of the level of suspicion being determined by arbitrary analogies, reasonableness should depend on whether the border exception makes sense in the context of files on a computer. The files on a laptop do not have the capacity to contain items that justify suspicionless searches at the border.

Several authors have criticized the application of the border exception to outbound travelers, arguing that the rationale for the border exception does not support suspcionless exit searches.[86] Although the Supreme Court has not addressed the validity of exit border searches, the lower courts have stated that the purpose is to search for exportation of money, which is related to the importation of drugs, and weapons.[87] First, this has been criticized because the fact that an outgoing container is brought into contact with the border should not render the border exception applicable because there is no "nexus between the search and the border."[88] Second, the border exception should not be used to transform a search that would be impermissible inland into a permissible one at the border when the need is no greater at the border than anywhere within the country.[89] As discussed, similar criticisms can be said about the application of the border exception to electronic storage devices. However, it is even more interesting that courts felt the need to connect export searches to the importation of drugs—the courts do not just claim that the border is a special place where a person's rights disappear.

2. The Search of Electronic Files Falls Outside the Scope of a Reasonable Border Search

The reasonable scope of a suspicionless border search should be limited not only by intrusiveness, but also by whether the invasion is supported by the rationale of the border exception. All searches under the Fourth Amendment, whether authorized by a warrant, probable

85. *See* 663 F.2d 1, 3 (2d Cir.1981).

86. *See, e.g.*, Nancy L. Dzwonczyk, *Criminal Procedure—Application of the "Border Search" Exception to Existing Individuals*—United States v. Ezeiruaku, 936 F.2d 136 (3d Cir. 1991), 65 Temp. L. Rev. 309, 318 (1992); Harris J. Yale, *Beyond the Border of Reasonableness: Exports, Imports, and the Border Exception*, 11 Hofstra L. Rev. 733, 770–71 (1983).

87. *See, e.g.*, United States v. Odutayo, 406 F.3d 386, 391 (5th Cir. 2005); United States v. Beras, 183 F.3d 22, 26 (9th Cir. 1999); United States v. Ezeiruaku, 936 F.2d 136 (3d Cir. 1991).

88. Yale, *supra* note 86, at 22.

89. *Id.*

cause, or pursuant to an exception, must be limited in scope to the circumstances which justify the intrusion in the first place. In *Terry v. Ohio*, the court upheld a protective search of a person's outer clothing based on reasonable suspicion and the scope was limited to what justified the exception in the first place, "the protection of the police officer and others nearby;" therefore, the scope of the search was confined to "an intrusion reasonably designed to discover guns, knives, clubs, or other hidden instruments for the assault of the police officer."[90]

Although searches at the border are unique based on the long standing "plenary authority" of the executive, the permissible scope of a routine border search should similarly be limited to what justifies the suspicionless search at the border. The purpose of the border exception should not be expanded to justify purely informational searches, beyond identification of the individual seeking entry because the government's interest in searching data and information is lower,[91] and there is no greater need to search computers at the border than anywhere else already in the United States. The government may "engage in suspicionless border searches where there is an interest unique to the border, such as preventing people from entering illegally or in intercepting drugs or weapons being brought into the country"; however, "these interests do not exist with regard to the memory of computers."[92] Other than the location where the search would take place, the search of laptop files has little to do at all with the borders; there is nothing exceptional or dangerous about information, ideas, and data being physically carried across the border on a hard drive that makes it more reasonable to search than the same data, located on the same hard drive, on your desk at home.

Although the exception has evolved from a purely financial interest, the purpose should not be expanded to include general law enforcement and uncovering terrorist materials without suspicion. Searches of a traveler's car, purse, briefcase, and luggage are consistent with the reasonable justifications of a border search. Taking a laptop out, and making sure that it doesn't contain explosives or contraband is also consistent. Even some things classified as nonroutine, for privacy reasons, are consistent with this rationale; drugs can be hidden in a person's cavity. However, clicking through the files on a laptop, and reading documents and emails falls outside the reasonable purpose of the border exception because "[t]he government has no special interest at the border in searching a person's computer different from computers that are

90. *See* 392 U.S. 1, 30 (1968).

91. Discussed *infra* Part V.A.

92. Erwin Chemerinsky, *Laptop Search at Border Was Illegal*, L.A. DAILY J., Nov. 29, 2006, at 6.

already in the country."[93]

The way that courts treat the scope of searches of electronic devices in other Fourth Amendment exceptions is informative. A search incident to a lawful arrest permits an officer to search the arrestee's person and the area within the arrestee's immediate control without a warrant in order to remove weapons and to prevent the concealment or destruction of evidence.[94] Although no federal case has addressed the validity of a computer search incident to arrest, several have addressed the search of cell phones incident to arrest. Courts have reached different decisions on whether a search incident to arrest extends to the contents of a cell phone. One court held that a search incident to arrest did not extend to cell phones where the defendant was arrested for driving on a suspended license and the officers smelled marijuana.[95] The court stated that the search was not related to officer safety or the preservation of evidence related to the crime of the arrest, but was instead a fishing expedition for evidence of drug activity.[96] Another court stated that cell phones may not be searched incident to arrest, as the contents of a cell phone present no risk of danger to arresting officers, and because "searching through information stored on a cell phone is analogous to a search of a sealed letter, which requires a warrant."[97] Many courts, on the other hand, have upheld the search of a cell phone incident to arrest; those cases reasoned that there was a risk that evidence would be destroyed because incoming calls would crowd out existing ones.[98] The treatment of the search of electronic devices incident to arrest is limited to what justifies the exception in the first place. Suspicionless searches of the same devices at the United States border should similarly require some relationship to the reasonable justifications for the border exception.

In a case regarding a warrant served on Google for the search of an e-mail account, a district court held that it did not comply with the Warrants Clause because it was too general; there was no provision limiting the emails to be seized to those containing evidence of the crimes

93. *Id.*

94. *See* Chimel v. California, 395 U.S. 752, 762–63 (1969).

95. United States v. Quintana, 594 F. Supp. 2d 1291, 1300 (M.D. Fla. 2009).

96. *See id.* (finding the search of cell phone incident to arrest improper because the search "had nothing to do with officer safety or the preservation of evidence related to the crime of arrest," but rather was a fishing expedition for evidence of drug activity).

97. *See* United States v. Wall, No. 08-60016-CR., 2008 WL 5381412, at *3 (S.D. Fla. Dec. 22, 2008).

98. *See* United States v. Murphy, 552 F.3d 405, 411 (4th Cir. 2009); United States v. Finley, 477 F.3d 250, 259–60 (5th Cir. 2007); United States v. Ortiz, 84 F.3d 977, 984 (7th Cir.1996); United States v. Santillan, 571 F. Supp. 2d 1093, 1102 (D. Ariz. 2008).

charged or of any specific crime at all.[99] Without the scope of border searches being limited to the justification of the border search doctrine, the exception seems similar to general warrants—the concern that underlies the Fourth Amendment in the first place.[100] Under general warrants "customs officials were given blanket authority to conduct general searches for goods imported to the Colonies in violation of the tax laws of the crown."[101] The Fourth Amendment rejects the use of general warrants by requiring that a warrant "particularly describe the place to be searched and the persons or things to be seized."[102] The district court quoted *United States v. George*, stating that "authorization to search for 'evidence of a crime,' that is to say, any crime, is so broad as to constitute a general warrant. . . . [A] fortiori, a warrant not limited in scope to any crime at all is . . . unconstitutionally broad."[103] Similarly, if the search of property is not limited in scope at the border, suspicionless searches of files contained within a laptop would be analogous to what the Fourth Amendment was designed to protect against: general warrants.[104]

B. *The Border Search of Laptop Files Only Serves General Law Enforcement Purposes*

The border search doctrine should not be used "for a purpose unrelated to border control—such as general crime prevention . . . ."[105] Customs officials are not subject to the same Fourth Amendment requirements as general law enforcement officers specifically because "[t]he primordial purpose of a search by Customs officers is not to apprehend persons, but to seize contraband property unlawfully imported or brought into the United States."[106] Therefore, the reason that customs officials can generally act without any level of suspicion is because "customs officials have special limited powers to enforce the *customs laws*; they do not have the general investigatory or law enforcement authority of police officers."[107]

---

99. *See* United States v. Cioffi, No. 08-CR-415 (FB), 2009 WL 3738314, at *9 (E.D.N.Y. Nov. 2, 2009).

100. *See* Berger v. New York, 388 U.S. 41, 58 (1967).

101. *Id.*

102. U.S. CONST. amend. IV.

103. *Cioffi*, No. 08-CR-415 (FB), 2009 WL 3738314, at *5 (E.D.N.Y. Nov. 2, 2009) (quoting United States v. George, 975 F.2d 72, 76–77 (2d. Cir. 1992)).

104. *See, e.g.*, Virginia v. Moore, 553 U.S. 164, 168–69 (2008) (citing Boyd v. United States, 116 U.S. 616, 624–27 (1886)).

105. United States v. Seljan, 547 F.3d 993, 1015 (9th Cir. 2008) (Kozinski, C.J., dissenting).

106. United States v. Sahanaja, 430 F.3d 1049, 1053 n.1 (9th Cir. 2005); Alexander v. United States, 362 F.2d 379, 382 (9th Cir. 1966).

107. Klein v. United States, 472 F.2d 847, 849 (9th Cir. 1973); People v. LaPiera, 611 N.Y.S.2d 394, 398 (N.Y. App. Div. 1994) (emphasis added).

However, the Department of Homeland Security sees the role of customs differently; explaining that searches of electronic media are "vital to detecting information that poses serious harm to the United States, including terrorist plans, *or constitutes criminal activity.*"[108] The role of the customs officer seems to be expanding and is becoming more difficult to distinguish from general law enforcement. The border should not be just a special place where the government has a good excuse to rummage around in people's stuff in hopes of finding anything that violates any kind of law without being subject to traditional Fourth Amendment requirements.

1. The Dangers of Using the Border Exception for General Law Enforcement

Allowing customs officials to have free access to every file on a traveler's computer will likely result in the border exception being used as an excuse to snoop computers for reasons unrelated to customs laws. The same court that upheld the suspicionless search of Arnold's laptop stated, in *United States* v. *Bulacan*, that "courts must take care to ensure that [a suspicionless] search is not subverted into a general search for evidence of crime," emphasizing the "vast potential for abuse" and intrusion "into the privacy of ordinary citizens."[109] Furthermore, the government has the same need to search data at the border as it does to search data inside computers already in the United States. "In the context of searching a laptop's data, the doctrine would require the existence of something special about searching the data *at* the physical border relative to searching data in computers already inside the country."[110] Searching for possession of things like copyright infringement[111] is no more necessary at the border than it is anywhere else in the United States.

2. Border Searches are Comparable to "Special Needs" Searches

Border searches have evolved in a way that makes them similar to suspicionless "special needs" searches. Under the "special needs" doctrine, suspicionless searches may be conducted when the government's

108. Press Release, Department of Homeland Security, Secretary Napolitano Announces New Directives on Border Searches of Electronic Media (Aug. 27, 2009), http://www.dhs.gov/ynews/releases/pr_1251393255852.shtm (emphasis added).

109. 156 F.3d 963, 967 (9th Cir. 1998).

110. 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, 255 (2008).

111. Press Release, *supra* note 108.

interest, beyond the normal need for law enforcement, outweighs the individual's privacy interest.[112] This means the government must state a reason for conducting the search that is separate from criminal law enforcement in order for the "special needs" doctrine to apply. Those searches are also not blanket searches, but are limited in scope to a specific goal.[113] Because the border exception has expanded beyond the need to regulate duties to include national security interests and importation of contraband[114], the Court created a balancing test, similar to the "special needs" test in order to distinguish between routine and nonroutine searches. However, unlike "special needs" searches, the balancing test at the border does not seem to be limited, in practice, to searches that are separate from general law enforcement, and searches at the border are not limited to the justifiable scope of the justified intrusion.

C. *The Utility of Laptop Searches Undermines the Application of the Border Exception*

The government's interest in searching the files on a laptop at the border is lower because the same data contained within every laptop can float across the border via the internet; therefore, border searches aren't that effective in preventing "dangerous data" from entering the United States. The lack of utility of such searches demonstrate how the border exception is being used as an excuse to do general crime searches without justification. The changes in the justification for the border exception have historically reflected newly perceived threats where the border is the rational point of defense.[115] However, information does not need to be carried across the physical border in order to enter the United States. Intercepting data, such as evidence of a terrorist plot, child pornography, or financial records at the nation's border cannot prevent its entry into the United States. Any terrorist can e-mail files across the border without having to physically transport them across the United States border and be protected by the Fourth Amendment. Illegal photos or other informational contraband will still enter the United States due to the nature of electronic communications.

Furthermore, this policy has the potential to extend to international e-mail. In deciding that the border exception should apply to international mail, the Supreme Court stated that "there is nothing in the rationale behind the border-search exception which suggests that the mode of

112. Ferguson v. Chalreston, 532 U.S. 67, 76 n.7 (2001).

113. *Id.* at 79.

114. *See supra* note 80 and accompanying text.

115. *Id.*

entry will be critical."[116] This makes it even more plausible that the border exception will encompass things like international e-mail, a far departure from what justifies the exception in the first place. One author even argued that "if the constitutional protections against unreasonable search and seizure, the right to due process, and other individual rights are not considered to be abrogated in physical border inspections, then it seems reasonable that appropriately narrow Internet border inspections should also survive a constitutional test."[117]

V. ELECTRONIC FILES CAN ONLY CONTAIN DATA AND INFORMATION WHICH UNDERMINES THE REASONABLENESS OF SEARCHING AT THE BORDER

Even at the border, the Fourth Amendment is incompatible with suspicionless informational searches. The border search doctrine has historically authorized extensive and highly discretionary searches. In the past, however, travelers had never carried an item across the border that was *only* capable of containing data and information, a characteristic that makes laptops significantly distinguishable from ordinary containers. Most containers, and indeed even bodily cavities, may be immediately dangerous to the United States because of their ability to conceal dangerous tangible items, not because of the information they contain. Information, by its nature, presents less of an immediate threat than ordinary objects. Many authors and courts have found that a laptop is not distinguishable in any way from other containers, one author argued that:

> laptop searches are not unique in their ability to reveal sensitive, personal information. Travelers might cross the border with letters, address books, photo albums, and similar items. . . . 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.[118]

Photo albums, journals, novels and other First Amendment materials are all capable of concealing drugs or weapons—a file on a computer or a Blackberry is not. Even a person's cavity—a search of which requires reasonable suspicion—is capable of containing drugs while a file on a computer never could. Computers are not only unique in the

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

117. Captain Oren K. Upton, Asserting National Sovereignty in Cyberspace: The Case for Internet Border Inspection (June 2003) (unpublished M.A. thesis, Naval Postgraduate School), http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA417582&Location=U2&doc=getTRDoc.pdf.

118. Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. RICH. L. REV. 1091, 1115 (2009).

information and data they contain—they are unique in their inability to contain anything other than information and data.

Because the distinction between routine and nonroutine searches turns on privacy and intrusiveness in order to require some level of suspicion, laptops must either be more like an extension of private body parts or a home. Instead courts have found it is more like a suitcase. The problem with these arguments is that it is not about how much data, or what kind of data a laptop contains—it is simply that it is data. The authority to search a laptop at the border should not depend on whether it is similar enough to a small list of things that judges consider to be sufficiently private at the border; it should turn on whether it is reasonable to search for information that has little to do with customs laws at the border. The authority to open a laptop to search for physical objects without suspicion should not extend to the information contained within the laptop.

A. *The First Amendment and Border Searches of Expressive Material*

The history of the border search exception illustrates that the doctrine was not initially intended to eliminate Fourth Amendment protections of personal papers. In *Boyd*, the case which courts have cited to support the historical strength of the border search doctrine,[119] the Supreme Court stated that "the search for and seizure of stolen or forfeited goods, or goods liable to duties and concealed to avoid the payment thereof, are totally different things from a search for and seizure of a man's private books and papers for the purposes of obtaining information therein contained . . . ."[120] The Constitution protects the right to receive information and ideas,[121] which is "fundamental to our free society."[122] The Supreme Court, in *New York v. P.J. Video*, refused to require a higher standard of probable cause for warrant applications when expressive material is involved, holding "an application for a warrant authorizing the seizure of materials presumptively protected by the First Amendment should be evaluated under the same standard of probable cause used to review warrant applications generally."[123]

Relying on *P.J. Video*, the Fourth Circuit then refused to create a First Amendment exception to the border search doctrine because it

119. *See, e.g.*, United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985).

120. Boyd v. United States, 116 U.S. 616, 623–24 (1886).

121. Griswold v. Connecticut, 381 U.S. 479, 482 (1965); Martin v. City of Struthers, 319 U.S. 141, 143 (1943).

122. Stanley v. Georgia, 394 U.S. 557, 564 (1969).

123. New York v. P.J. Video, 475 U.S. 868, 874 (1986).

believed that the Supreme Court had foreclosed this argument.[124] In *United States v. Arnold*, the Ninth Circuit affirmed the Fourth Circuit's reasoning that such a rule would:

> (1) protect terrorist communications "which are inherently 'expressive' "; (2) create an unworkable standard for government agents who "would have to decide-on their feet-which expressive material is covered by the First Amendment"; and (3) contravene the weight of Supreme Court precedent refusing to subject government action to greater scrutiny with respect to the Fourth Amendment when an alleged First Amendment interest is also at stake.[125]

Other federal circuits addressing this issue have also held that expressive materials are not exempt from the border search exception.[126] First, requiring reasonable suspicion in order to conduct a search of laptop files at the border may have the effect of sometimes protecting terrorist communications; however, this justification is insufficient. The argument has turned up elsewhere, such as in *Flores-Montano*, where the Government argued that if a trunk can be searched without reasonable suspicion but a gas tank cannot be, it will encourage terrorists to hide materials in the gas tank.[127] But this argument is rejected elsewhere. First of all, terrorists could also hide materials in their cavities, or send the materials to themselves through the U.S. Postal Service, or via the Internet.[128] In *United States v. United States District Court*, the Court addressed wiretaps that were used against citizens who were suspected of conspiracy to bomb government property.[129] The Supreme Court balanced the government interest to protect national security against the invasion on individual privacy and unanimously found that some Fourth Amendment safeguards were still necessary.[130] Searching the files on a laptop is similar to wiretapping because it is limited to ideas, information and communications that can travel through the air waves.

Second, the Supreme Court's holding did not foreclose a First Amendment defense to a border search. A suspicionless search pursuant to a Fourth Amendment exception involves a different analysis than a warrant application; it involves a balance of the government's interest against the individual's interest. Because the reasonableness requirement applies at the border, the interest in protecting the free flow of ideas

---

124. *See* United States v. Ickes, 393 F.3d 501, 507 (4th Cir. 2005).

125. United States v. Arnold, 533 F.3d 1003, 1010 (9th Cir. 2008).

126. *See* United States v. Seljan, 547 F.3d 993, 1011 (9th Cir. 2008); Tabbaa v. Chertoff, 509 F.3d 89, 102 (2d Cir. 2007).

127. Brief for the United States at 18, United States v. Flores-Montano, 541 U.S. 149 (2004) (No. 02-1794).

128. Discussed *infra* Part V.B.

129. *See* 407 U.S. 297, 323–24 (1972).

130. *See id.* at 313.

should weigh in favor of the individual's interest to be balanced against the government interest. The strong weight of the individual's interest in protecting the free flow of information is reflected in border cases outside the context of laptops where courts seem to treat information searches at the border with more caution than other items at the border.

Several courts have found that once a search of an envelope or package reveals no contraband or dutiable items, a close reading or photocopying of the contents of documents requires reasonable suspicion.[131] Courts have also upheld a limited reading or examination of documents found during a border search, but only to identify the objects themselves,[132] while emphasizing that "a reading for the purpose of revealing the *intellectual content* of the writing requires encroachment upon first amendment protections far beyond the mere search and seizure of materials."[133] This caution exhibited by the courts reveals an implicit regard for, or fear of invading, individual's First Amendment rights at the border.

Third, requiring suspicion in order to search a laptop at the border would not create an "unworkable standard" for officials because it is not necessary to exempt all expressive materials from searches at the border in order to protect the files on a computer. The requirement of reasonable suspicion could be limited to items that are only capable of containing data and information. It is clear that officials may open a laptop, journal, or photo album to inspect for physical objects, and even turn on a laptop to make sure it isn't a bomb without suspicion, but that authority should not extend to information contained within these items. The government's interest in searching laptops at the border is attenuated because of the futility of searching the contents of a laptop at the border, and because the purpose of the border exception is not to reveal content of writings. Therefore, because travelers' First Amendment interest in the free flow of information weighs against the government, reasonable-

131. *See, e.g.*, United States v. Fortna, 796 F.2d 724, 738–39 (5th Cir. 1989) (upholding photocopying of documents and a map found in a carry-on bag during a border search because the documents aroused the agents' suspicion of illegal conduct involving material or persons entering or leaving the United States); United States v. Grayson, 597 F.2d 1225, 1229 (9th Cir. 1979) (stating that where the defendant reluctantly removed papers from his breast pocket and crumbled them after being asked by customs officials to empty his pockets, "such actions gave the inspectors reason to suspect that the papers contained or related to contraband or were evidence of items not declared by the defendant; this required that the papers be read"); United States v. Schoor, 597 F.2d 1303, 1306 (9th Cir. 1979) (holding that air cargo bills and other documents were properly seized by custom officials upon notification that items were instrumentalities of crime involving narcotics); United States v. Soto-Teran, 44 F. Supp. 2d 185, 191 (E.D.N.Y.1996). *But see* United States v. Borello, 766 F.2d 46, 58 (2d Cir.1985) (holding customs officials may screen materials to enforce obscenity laws without violating the First Amendment).

132. *See, e.g.*, Heidy v. U.S. Customs Serv., 681 F. Supp. 1445, 1450 (C.D. Cal. 1988).

133. *See id.*

ness requires that customs officials have some level of suspicion before searching devices that are only capable of containing data and information.

B. *Data and Information in International Mail*

Historically, the suspicionless reading of personal information and correspondence would have been considered unreasonable. In 1792, Congress made it a crime for Post Office employees to open any letter, packet, or bag of letters.[134] In 1866, Congress broadened the authority of Customs officials to allow a search of "any vessel, beast, person or *envelope* without suspicion."[135] There were concerns that the use of the word "envelope" would be interpreted to allow inspection of personal correspondence; however, the sponsor assured that "[t]here is no danger of such a construction being placed upon this language."[136]

In *United States v. Ramsey*, the Supreme Court held that the same constitutional standard should be applied regardless whether the item is carried across the border, or crosses the border through international mail.[137] Under 19 U.S.C. § 1583, customs officials are required to have reasonable cause to suspect that an item contains contraband before opening sealed envelopes carried by the U.S. Postal Service, and they are flatly prohibited from reading correspondence in the absence of a search warrant.[138] Additionally, 19 C.F.R. § 145.3 prohibits customs officials from reading correspondence contained in "any letter class mail" absent prior authorization by search warrant or by written authorization of the sender or the recipient. In *Ramsey*, the Supreme Court declined to address whether customs inspectors could read correspondence because "the reading of letters is totally interdicted by regulation,"[139] meaning, the statute that applied to the search conducted in the case already required reasonable suspicion, which the inspectors had.[140]

The Ninth Circuit became the first court to uphold the supsicionless reading of international correspondence in *United States v. Seljan.*[141] The Court held that the scope of a search of international mail, authorized under 31 U.S.C. § 5317, was reasonable where the inspector

134. An Act to establish the Post-Office and Post Roads within the United States, 1 Stat. 232, sec. 5 (1792).

135. Act of July 1866, 14 Stat. 178 § 2.

136. *See* United States v. Ramsey, 431 U.S. 606, 627 (1977) (Stevens, J., dissenting) (quoting Cong. Globe, 39th Cong., 1st Sess., 2596 (1866)).

137. *Id.* at 620.

138. 19 U.S.C. § 1583(c)(2) (2010).

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

140. *Id.*

141. 547 F.3d 993, 1003 (9th Cir. 2008).

opened the package and "scanned" the letter to determine whether defendant had violated monetary instrument reporting requirements, and evidence of pedophilia could be ascertained "by a glance."[142]

The Ninth Circuit—the same court that upheld the suspicionless search of Arnold's computer less than four months earlier—seemed to exercise extreme caution when dealing with a postal inspector reading contents of communications. The court stated that it was necessary to unfold the paper and look at what was printed on it in order to determine whether it was a monetary instrument.[143] The court repeatedly emphasized that the inspector did not "read" the letter, but instead "scanned" it, relying on the plain view doctrine to find it was reasonable.[144] Under the plain view doctrine, if officers are lawfully in a position where they see an object, the object's incriminating character is immediately apparent and if the officers have lawful right of access to the object, they may seize it without a warrant.[145] "The initial intrusion can be justified by a warrant or by one of the recognized exceptions of the warrant requirement."[146] The court stated that the cursory "scanning" of the letter fell under the plain view doctrine because the border exception gave the official a lawful vantage point to open the letter, and the inspector noticed "immediately apparent" evidence of pedophilia.[147]

The court implicitly recognized the scope of the border search was limited by the purpose of the initial intrusion—to identify the letter itself—and was not supposed to extend to private communications. First, the court's emphasis on the inspector's method of "scanning," as opposed to reading, the information reveals a special caution the court seems to afford the reading of information, even at the border. The court also emphasized that the purpose of the search was not to read the information, but that the information was in plain view and immediately apparent as contraband. If the border exception justified the reading of communications, the court would not have had to rely on the plain view doctrine to find the search was reasonable.

Similarly, when customs officials search a physical diary or photo album, they are not supposed to be searching them for intellectual content; they are searching for contraband contained within the item. However, if customs officials come across other items during their search for contraband, they are authorized to seize it. If the same standard is supposed to apply to physical border searches, and border searches of inter-

142. *Id.* at 1004–05.
143. *Id.* at 1004.
144. *Id.* at 1005.
145. *See* Minnesota v. Dickerson, 508 U.S. 366, 374–75 (1993).
146. Horton v. California, 496 U.S. 128, 136 (1990).
147. United States v. Seljan, 547 F.3d 993, 1006 (9th Cir. 2008).

national mail, why did the Ninth Circuit feel compelled to be more protective over information contained within a piece of mail than information contained within a laptop?

Although data on a laptop is probably most closely analogous to a piece of international mail because they are both likely to contain private information, ideas, and communications, there are some key differences which would implicate that the suspicionless search of a laptop at the border is even less justified than the search of international mail. First, a letter is similar to other closed containers that are capable of storing physical items, and laptop files can only store data and information. Second, the Ninth Circuit, in *Seljan*, relied heavily on the plain view doctrine to justify the cursory scanning of correspondence.[148] The same rationale cannot support the search of files within a laptop because when the physical laptop itself is searched, electronic files do not come into plain view. Although the plain view doctrine might come into play when a laptop is booted up to identify the object itself, it would be limited to things that are immediately apparent as contraband on the desktop—a much more limited scope than perusing all of the files. For example, customs officials would be justified in turning on Arnolds computer to make sure it wasn't a bomb; therefore if his desktop picture depicted child pornography or maybe if the files on the desktop had been entitled "nude kids" or "child porn" instead of "Kodak memories,"[149] it may have fallen under the plain view doctrine. It would be interesting to see how the Ninth Circuit would decide a case in which a laptop was sent through international mail. Although the court's decision in *United States v. Arnold* would seem to allow a suspicionless search of all of the files,[150] the court's decision in *Seljan* would seem to limit the search to information in plain view,[151] which, in the case of a laptop could only extend to information immediately apparent as contraband on the desktop. The protection of international correspondence provided by statute combined with the caution exhibited by the only court to have upheld the suspicionless "scanning" of correspondence undermine the approval of customs officials reading information on a laptop. It does not seem logical that the courts can say that the same standard should apply to international mail and information physically traveling with a person across the border, and at the same time give more protection to information in international mail than information contained within a laptop.

148. *See id.* at 1006.

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

150. *See id.*

151. *See Seljan*, 547 F.3d at 1006.

VI. CONCLUSION

Some level of individualized suspicion should be required before customs officials can search the electronic contents of a laptop. The purpose of the border exception to the Fourth Amendment does not support the suspicionless searches of electronic storage devices. Although the justifications for the exception have evolved, it should not be extended to a search that has little to do with physically crossing the border and that is, by its nature, less dangerous than physical objects. The government's interest in the search of information on a laptop at the border is attenuated because there is no greater need to search information on a laptop at the border than anywhere else in the country, and because electronic files can be e-mailed across the border. The individual's interest in the free flow of information weighs against the government's already lower interest in searching. Courts have exhibited caution in dealing with the suspicionless reading of personal information in both First Amendment cases as well as cases involving international mail, which exemplifies courts' acknowledgement of this interest. Furthermore, the Ninth Circuit's reliance on the plain view doctrine in *Seljan* undermines its holding in *Arnold*. The rationale for the border search exception does not justify the suspicionless search of laptops and other electronic storage devices, which is one of the reasons why travelers, who are accustomed to their lowered privacy interest at the border, are surprised the officers can search their laptop. A border search that falls outside the scope of the reasonable justifications for the border exception, is attenuated from the government's interest at the border, and one that involves property that can only contain personal information and data cannot be considered routine.