

NOTES

SHOULD YOU LEAVE YOUR LAPTOP AT HOME WHEN TRAVELING ABROAD?: THE FOURTH AMENDMENT AND BORDER SEARCHES OF LAPTOP COMPUTERS

RASHA ALZAHABI*

INTRODUCTION

Technologies permeate every aspect of our lives. From cellular phones and iPods to laptop computers and USB keys, hardly anyone walks down the street without carrying at least one of these items. The various uses of new technologies often impact our legal rights and raise new issues with which courts must grapple.¹ One such issue exists when people travel through our country's airports. Since the tragic events of September 11, 2001, the government has noticeably revamped security at airports. But what are the limits? When does an airport official's conduct cross the line?

The Fourth Amendment guarantees “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,” and that “no Warrants shall issue, but upon probable cause.”² Thus, searches conducted without a warrant are “per se unreasonable,” save a few

* J.D. Candidate, 2008, Indiana University School of Law—Indianapolis; B.A., 2005, Indiana University Purdue University—Indianapolis. Recipient of the Papke Prize for Best Note in Volume 41, endowed by and named in honor of David R. Papke, former R. Bruce Townsend Professor of Law and faculty advisor to the Indiana Law Review.

I would like to thank my parents, Basem Alzahabi and Sana Alomary, without whom I would not be the person I am today, and my husband, Waddah Maskoun, without whose patience and support this Note and my success in law school would not be possible. I am also thankful to Professor and Dean Emeritus Norman Lefstein for his insightful and helpful suggestions throughout the writing of this Note. Finally, I would like to thank Professor Orin Kerr of the George Washington University Law School for his posting on The Volokh Conspiracy that was the inspiration for this Note topic. See Posting of Orin Kerr to The Volokh Conspiracy, <http://volokh.com/posts/1160582029.shtml> (Oct. 11, 2006, 11:53 EST).

1. See, e.g., *Kyllo v. United States*, 533 U.S. 27, 29 (2001) (deciding whether the use of a thermal-imaging device to detect heat inside of a home constituted a “search” under the Fourth Amendment); see also Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 280 (2005) (“Digital evidence should trigger new rules of criminal procedure because computer-related crimes feature new facts that will demand new law.”).

2. U.S. CONST. amend. IV.

enumerated exceptions.³ One such exception applies at our nation's borders.⁴ Therefore, under what is known as the "border search exception," a customs official may search travelers and their luggage at the border without a warrant or probable cause.⁵ But what about the files saved on a traveler's laptop computer or USB key? Is the laptop computer akin to a suitcase or a purse? Or is it like a body cavity, which may not fall within the border search exception?⁶ Numerous courts have addressed this issue⁷ but have yet to reach a consensus on how to deal with it. Most recently, in *United States v. Arnold*,⁸ a federal district court held that in order for a border search of information contained in a laptop or other similar storage device to be constitutional, it must be sparked by at least reasonable suspicion.⁹ Earlier cases seemed to take a different approach, granting airport officials greater latitude in conducting laptop searches at the border.¹⁰

3. *Katz v. United States*, 389 U.S. 347, 357 (1967). Numerous commentators have suggested, however, that the so-called exceptions have practically swallowed the general rule. *See California v. Acevedo*, 500 U.S. 565, 582 (1991) (Scalia, J., concurring) ("[T]he 'warrant requirement' has become so riddled with exceptions . . . it [i]s basically unrecognizable."); Craig M. Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1473 (1985) (noting that the exceptions to the warrant requirement "are neither few nor well-delineated"); *see also* Wayne D. Holly, *The Fourth Amendment Hangs in the Balance: Resurrecting the Warrant Requirement Through Strict Scrutiny*, 13 N.Y.L. SCH. J. HUM. RTS. 531 (1997).

4. *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985).

5. *Id.* at 538. It is to be noted at the outset that this Note will only discuss the constitutionality of laptop searches *at the border*. Border searches include those searches conducted "when entry is made by land from the neighboring countries of Mexico and Canada, at the place where a ship docks in this country after having been to a foreign port, [and] at any airport in the country where international flights land." 5 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 10.5(a) (4th ed. 2004) (footnotes omitted). Airport searches fall within a different exception to the warrant requirement. *See generally id.* § 10.6. The standards and rules governing airport searches differ from those controlling the scope of border searches. *See id.* This is due, in part, to the different functions of the two categories of searches. *Compare id.* § 10.6(c) (quoting *United States v. Davis*, 482 F.2d 893 (9th Cir. 1973)) (stating that airport searches are conducted "to prevent the carrying of weapons or explosives aboard aircraft, and thereby to prevent hijackings"), *with id.* § 10.5(a) (quoting Judith B. Ittig, *The Rites of Passage: Border Searches and the Fourth Amendment*, 40 TENN. L. REV. 329, 331 (1973)) (stating that the purpose of border searches is "to identify citizenship, collect payment on dutiable goods, and prevent the importation of contraband").

6. *See Montoya de Hernandez*, 473 U.S. at 541 n.4 ("[W]e suggest no view on what level of suspicion, if any, is required for nonroutine border searches such as strip, body-cavity, or involuntary x-ray searches.").

7. *See, e.g., United States v. Romm*, 455 F.3d 990 (9th Cir. 2006), *cert. denied*, 127 S. Ct. 1024 (2007); *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005).

8. 454 F. Supp. 2d 999 (C.D. Cal. 2006).

9. *Id.* at 1007.

10. *See, e.g., Ickes*, 393 F.3d at 505 (affirming a laptop border search that was based on

Most of the searches at issue in the laptop cases have culminated in customs officials finding child pornography saved in the travelers' laptops, often leading to convictions under federal law.¹¹ However, these rulings have broader implications. "People keep all types of personal information on computers, including diaries, personal letters, medical information, photos and financial records;"¹² thus, if an airport or customs official may search laptop files without reasonable suspicion or probable cause, people may hesitate to store such information on their laptops, or even to carry their laptops onto airplanes when traveling to other countries. Attorneys and businessmen, who may store confidential client information on their laptops, are especially affected by these rulings.¹³

This Note analyzes whether it is constitutional for laptop computers to be searched at the border without any level of suspicion. In Part I, this Note discusses the Fourth Amendment and the border search exception generally. Part II discusses the relevant case law dealing with border searches of laptops and the implications of these rulings. Part III argues that laptop searches at the border should not be considered routine border searches and, thus, should be based on, at the least, reasonable suspicion to be constitutional. Specifically, this section argues that laptop border searches are inconsistent with the traditional rationales that justify the border search exception; that the search of a laptop is more than a "relatively limited intrusion;" and that travelers' strong privacy interests in their laptops outweigh the government's interest in conducting suspicionless laptop border searches. Part IV discusses two important cases in Fourth Amendment jurisprudence involving new laws formulated as a result of the impact of new technologies. Part V addresses the practical implications of the recent rulings allowing airport personnel to conduct suspicionless laptop border searches. This Note concludes that in light of the reliance people have on their laptops and other technologies, a clear rule in this area is needed – a rule that reassures travelers that the files on their laptops will not be searched without, at the least, reasonable suspicion.

reasonable suspicion, but suggesting that the search was reasonable simply because it took place at the border).

11. See, e.g., *Romm*, 455 F.3d at 993 (concerning a defendant convicted of knowingly receiving and possessing child pornography); *Ickes*, 393 F.3d at 502 (concerning a defendant convicted of transporting child pornography). While not all Fourth Amendment cases deal with pornography, they do usually deal with criminals; as Justice Frankfurter once stated: "It 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. Arnold*, 454 F. Supp. 2d 999, 1004 (C.D. Cal. 2006) (quoting *Montoya de Hernandez*, 473 U.S. at 548 (Brennan, J., dissenting)).

12. *Arnold*, 454 F. Supp. 2d at 1003-04.

13. See Steve Seidenberg, *9th Circuit: Laptops May Be Subject to Customs Inspections After Overseas Trips*, 5 NO. 37 A.B.A. J. E-REP. 4 (2006) (warning lawyers of the "bind" they may find themselves in).

I. AN ANALYSIS OF THE FOURTH AMENDMENT AND THE BORDER SEARCH EXCEPTION

Understanding the Fourth Amendment generally, as well as the border search doctrine, is necessary when analyzing whether suspicionless laptop border searches are constitutional.¹⁴ The Fourth Amendment, protecting us from “unreasonable searches and seizures,” was designed to deter police misconduct and is an important safeguard against intrusions on our privacy and possessory rights.

A. *The Fourth Amendment Generally*

The Fourth Amendment states that “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause”¹⁵ While the general rule is that searches conducted without a warrant are “per se unreasonable,”¹⁶ there are a number of important exceptions to this warrant requirement.¹⁷ For some of these exceptions, probable cause is required for the search to be constitutional.¹⁸ Other exceptions allow searches to be conducted based upon a standard lower than probable cause, referred to as “reasonable suspicion.”¹⁹ Reasonable suspicion is defined as “individualized suspicion . . . less compelling than is needed for the usual law enforcement search.”²⁰ Finally, some searches don’t require a warrant, probable cause, or any

14. Considering that Fourth Amendment law has been referred to as “confusing,” Bradley, *supra* note 3, at 1472, “a mass of contradictions and obscurities,” *id.* at 1468, and “unstable and unconvincing,” *id.* at 1468 (quoting Lloyd L. Weinreb, *Generalities of the Fourth Amendment*, 42 U. CHI. L. REV. 47, 49 (1974)), this is no easy task.

15. U.S. CONST. amend. IV.

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

17. *See* Bradley, *supra* note 3, at 1473-74 (listing over twenty exceptions to “the probable cause or warrant requirement or both”).

18. *See, e.g., Carroll v. United States*, 267 U.S. 132, 162 (1925) (holding that a warrantless search of a car stopped by police officers who had probable cause to believe the vehicle contained contraband was not unreasonable); *see also United States v. Ross*, 456 U.S. 798, 825 (1982) (extending *Carroll* to “every part of the vehicle and its contents that may conceal the object of the search” as long as probable cause justifies the search of the stopped vehicle in the first place).

19. This standard was first articulated by the Court in *Terry v. Ohio*, 392 U.S. 1, 30 (1968), which held that a “stop” and “frisk” conducted by a police officer was constitutional because it was based on a reasonable suspicion that a “criminal activity may be afoot and that the persons with whom he is dealing may be armed and presently dangerous.” The reasonable suspicion standard was, later, extended to numerous other contexts. *See, e.g., O’Connor v. Ortega*, 480 U.S. 709 (1987); *New Jersey v. T.L.O.*, 469 U.S. 325 (1985); *see also* JEROLD H. ISRAEL ET AL., *CRIMINAL PROCEDURE AND THE CONSTITUTION: LEADING SUPREME COURT CASES AND INTRODUCTORY TEXT* 252 (2006).

20. ISRAEL ET AL., *supra* note 19, at 252.

level of suspicion to be constitutional,²¹ but are still governed by the reasonableness standard set forth in the Fourth Amendment.

The seminal case in modern Fourth Amendment jurisprudence is *Katz v. United States*.²² In *Katz*, the United States Supreme Court rejected the notion that a physical intrusion must occur into a constitutionally protected area for there to be a Fourth Amendment violation.²³ Rather, the Court stated, “[T]he Fourth Amendment protects people, not places,”²⁴ and found that government officials had violated the Fourth Amendment in the case at hand because they had infringed on the defendant’s justified expectation of privacy.²⁵

The Court elaborated on this test further when it stated in a later case: “The warrantless search and seizure of [the evidence] would violate the Fourth Amendment only if respondents manifested a subjective expectation of privacy [in the evidence] that society accepts as objectively reasonable.”²⁶ This sets forth a two-step test for whether a defendant has an expectation of privacy protected by the Fourth Amendment. First, the court must find that there was a subjective expectation of privacy. Second, the court must decide that the interest is one that society finds to be reasonable; in other words, one to which the court is willing to give Fourth Amendment protection. While this inquiry into the expectation of privacy of the defendant is relevant and important in the case of laptop searches at the border, and one to which we will return, it must be analyzed within the context of the border search doctrine.

B. *The Border Search Exception to the Fourth Amendment*

The border search is one of numerous administrative and regulatory searches,²⁷ a wide range of searches that may be conducted without a warrant or probable cause.²⁸ While some administrative searches require reasonable suspicion to be constitutional,²⁹ others, including the border search, require no suspicion whatsoever.³⁰ The idea behind this final category of searches requiring no suspicion is that they are “conducted pursuant to some neutral criteria which

21. This includes routine border searches, “airport security checks, driver’s license check roadblocks, and sobriety checkpoints.” *Id.*

22. 389 U.S. 347 (1967).

23. *Id.* at 353.

24. *Id.* at 351.

25. *Id.* at 353.

26. *California v. Greenwood*, 486 U.S. 35, 39 (1988).

27. See LAFAVE, *supra* note 5, § 10.5(a).

28. ISRAEL ET AL., *supra* note 19, at 252.

29. For instance, the Supreme Court upheld the search of a student in a public school based on reasonable suspicion of a violation of school rules in *New Jersey v. T.L.O.*, 469 U.S. 325 (1985), and the search of a government employee’s workplace for work-related reasons based on reasonable suspicion in *O’Connor v. Ortega*, 480 U.S. 709 (1987). ISRAEL ET AL., *supra* note 19, at 252.

30. See ISRAEL ET AL., *supra* note 19, at 252; LAFAVE, *supra* note 5, § 10.5(a).

guard[s] against arbitrary selection of those subjected to such procedures."³¹ In the case of border searches, the neutral criterion is that one has "entered into our country from outside."³² Border searches "may in certain circumstances take place not only at the border itself, but at its functional equivalents as well."³³ Numerous lower courts have held that border searches may also be conducted as travelers exit our country.³⁴

The border search exception dates back to the First Congress, which passed a customs statute exempting border searches from probable cause and warrant requirements.³⁵ Later, the United States Supreme Court elaborated on the border search exception as follows: "Since the founding of our Republic, Congress has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country."³⁶

1. *Camara v. Municipal Court of San Francisco*.—In *Camara v. Municipal Court of San Francisco*,³⁷ the United States Supreme Court upheld another "administrative search, the health and safety inspection of buildings."³⁸ The Court's reasoning in *Camara* "is equally applicable to the routine border search."³⁹ In *Camara*, the Court stated: "[T]here can be no ready test for determining reasonableness other than by balancing the need to search against the invasion which the search entails."⁴⁰ The Court went on to state that there are "a number of persuasive factors" that "combine to support the reasonableness of area code-enforcement inspections."⁴¹ The Court listed the factors as follows:

First, such programs have a long history of judicial and public acceptance. . . . Second, the public interest demands that all dangerous

31. ISRAEL ET AL., *supra* note 19, at 252.

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

33. *Almeida-Sanchez v. United States*, 413 U.S. 266, 272 (1973) (holding that a roving patrol search of a car twenty miles from the U.S.-Mexico border was *not* a border search). The Court listed "searches at an established station near the border, at a point marking the confluence of two or more roads that extend from the border . . . [, or] a search of the passengers and cargo of an airplane arriving at a St. Louis airport after a nonstop flight from Mexico City" as examples of searches taking place at the functional equivalent of the border. *Id.* at 273.

34. LAFAVE, *supra* note 5, § 10.5(a) n.10 (listing cases that have held such); *see, e.g.*, *United States v. Stanley*, 545 F.2d 661, 667 (9th Cir. 1976) (listing numerous features in-coming and out-going border crossing searches have in common).

35. LAFAVE, *supra* note 5, § 10.5(a) (citing Act of July 31, 1789, ch. 5, 1 Stat. 29).

36. *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985) (citing *Ramsey*, 431 U.S. at 616-17 (citing Act of July 31, 1789, ch. 5, 1 Stat. 29)).

37. 387 U.S. 523 (1967).

38. LAFAVE, *supra* note 5, § 10.5(a).

39. *Id.*

40. *Camara*, 387 U.S. at 536-37.

41. *Id.* at 537.

conditions be prevented or abated, yet it is doubtful that any other canvassing technique would achieve acceptable results. . . . Finally, because the inspections are neither personal in nature nor aimed at the discovery of evidence of crime, they involve a relatively limited invasion of the urban citizen's privacy.⁴²

These three factors explain why, in the Court's view, health and safety inspections of buildings were reasonable and did not require a warrant or any level of suspicion. Professor LaFave explains how this reasoning applies to the routine border search.⁴³ First, the border search "has a long history of judicial and public acceptance," similar to the health inspection of buildings, as demonstrated by the fact that border "searches were first authorized by the same Congress which proposed the Bill of Rights."⁴⁴ Second, there is "a strong public interest in effective preventive measures," specifically "to identify citizenship, collect payment on dutiable goods, and prevent the importation of contraband . . . [all of which] would be almost completely frustrated by the confines of a search warrant predicated on a showing of probable cause."⁴⁵ As to the last factor, while the routine border search is not as impersonal as the health or safety inspection of a building, it is "a relatively limited invasion"⁴⁶ because travelers crossing the border are on notice that the search may take place, and there is no stigma attached to the search.⁴⁷

The foregoing discussion only applies to routine customs searches and inspections. In other words, it is only when a search is a "relatively limited invasion" that the *Camara* balancing test justifies a border search merely on the basis that a person has crossed the border.⁴⁸ If the invasion is more intrusive, "there is a need to strike the balance anew."⁴⁹

2. *United States v. Montoya de Hernandez*.—In *United States v. Montoya de Hernandez*,⁵⁰ the United States Supreme Court addressed the question of "what level of suspicion would justify a seizure of an incoming traveler for purposes other than a routine border search."⁵¹ The defendant in *Montoya de Hernandez* was suspected of smuggling drugs across the border by hiding them

42. *Id.* (citation omitted).

43. See LAFAVE, *supra* note 5, § 10.5(a).

44. *Id.*

45. *Id.* (quoting Ittig, *supra* note 5, at 331).

46. *Camara*, 387 U.S. at 537.

47. LAFAVE, *supra* note 5, § 10.5(a).

48. *Id.*

49. *Id.* Professor LaFave explains that this is "illustrated by the established rule that a so-called strip search may be conducted only upon a 'real suspicion, directed specifically to that person.'" *Id.* (quoting *Henderson v. United States*, 390 F.2d 805 (9th Cir. 1967), but noting that other courts use a "reasonable suspicion" standard instead of the "real suspicion" standard).

50. 473 U.S. 531 (1985).

51. *Id.* at 540.

in her alimentary canal.⁵² She was detained by U.S. Customs at the Los Angeles airport for an extended period of time.⁵³ The next day, a warrant was obtained, authorizing a rectal exam and x-ray, which revealed that the defendant had a balloon of an illegal substance hidden in her alimentary canal.⁵⁴ She passed six more balloons that day and eighty-eight balloons, containing a total of 528 grams of cocaine, over the next several days.⁵⁵

The Supreme Court affirmed the conviction and held that detaining 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.”⁵⁶ Thus, the Court made it clear that the extended detention of the traveler was indeed a non-routine search, and held that such non-routine searches would need to be supported by reasonable suspicion to be constitutional.⁵⁷

The Court in *Montoya de Hernandez* emphasized, in a footnote, what it did not hold—“we suggest no view on what level of suspicion, if any, is required for nonroutine border searches such as strip, body-cavity, or involuntary x-ray searches.”⁵⁸ By this statement, the Court provided three examples of non-routine searches—strip searches, body cavity searches, and involuntary x-ray searches. All of these searches are more intrusive than a routine border search. Further, the Court left open the question of whether reasonable suspicion would be sufficient to justify such a search, or whether a higher standard would be required.⁵⁹

3. *United States v. Flores-Montano*.—In a recent case, the United States Supreme Court used language indicating it still retained the distinction between routine and non-routine searches. In *United States v. Flores-Montano*,⁶⁰ the Supreme Court held that “the Government’s authority to conduct suspicionless inspections at the border includes the authority to remove, disassemble, and reassemble a vehicle’s fuel tank.”⁶¹ The Court reversed the Ninth Circuit on this issue.⁶² The Ninth Circuit had based its ruling on one of its earlier cases, in which it had held that in “‘a search that goes beyond the routine, an inspector must have reasonable suspicion,’ and the ‘critical factor’ in determining whether

52. *Id.* at 534.

53. *Id.* at 533-35.

54. *Id.* at 535.

55. *Id.* at 536.

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

57. *See id.*

58. *Id.* at 541 n.4.

59. Lower federal and state courts have held, however, that for strip searches to be constitutional, they must be based on “reasonable suspicion.” PHILLIP A. HUBBART, MAKING SENSE OF SEARCH AND SEIZURE LAW: A FOURTH AMENDMENT HANDBOOK 288 (2005) (citing LAFAVE, *supra* note 5, § 10.5(c)).

60. 541 U.S. 149 (2004).

61. *Id.* at 155.

62. *Id.* at 156.

a search is ‘routine’ is the ‘degree of intrusiveness.’”⁶³

The Supreme Court stated: “[T]he reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person—dignity and privacy interests of the person being searched—simply do not carry over to vehicles.”⁶⁴ Further the Court stated: “Complex balancing tests to determine what is a ‘routine’ search of a vehicle, as opposed to a more ‘intrusive’ search of a person, have no place in border searches of vehicles.”⁶⁵ This is consistent with rulings in other cases that have constantly given us fewer rights in the context of car searches, especially when compared to physical searches or searches of the home.⁶⁶

In *Flores-Montano*, the United States Supreme Court decision resolved only a narrow issue, holding that extensive searches of cars at the border were routine and fell squarely within the border search exception and, thus, did not require any level of suspicion to be constitutional.⁶⁷ The Court did not provide explicit guidance on any other kind of search. However, by ruling that the search of a car is routine,⁶⁸ the Court implied that it retained the distinction between routine and non-routine searches, as set forth in *Montoya de Hernandez*.⁶⁹

Furthermore, the Court pointed to the interests at stake that may “support a requirement of some level of suspicion”—the “dignity and privacy interests of the person being searched.”⁷⁰ This analysis may parallel the inquiry set forth in *Katz* that is relevant when determining if a search has taken place. Thus, the question remains—are these interests at stake when a border official searches through the files of a traveler’s laptop computer?⁷¹ If this question is answered affirmatively, it may follow that the search of a laptop is non-routine and intrusive, and, therefore, requires at least some level of suspicion to be constitutional.

63. *Id.* at 152 (citing *United States v. Molina-Tarazon*, 279 F.3d 709, 712-13 (9th Cir. 2002)).

64. *Id.*

65. *Id.*

66. See ISRAEL ET AL., *supra* note 19, at 188.

67. See *Flores-Montano*, 541 U.S. at 155.

68. See *id.* at 153-55.

69. See *United States v. Montoya de Hernandez*, 473 U.S. 531, 541 n.4 (1985) (stating that “we suggest no view on what level of suspicion, if any, is required for nonroutine border searches such as strip, body-cavity, or involuntary x-ray searches.”).

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

71. This is not the first time new technologies have run the risk of intruding on our right to privacy, as was noted by Justice Scalia in *Kyllo v. United States*, 533 U.S. 27, 33-34 (2001), when he stated that “[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.” See generally Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004).

II. COURTS' RESPONSES TO SEARCHES OF LAPTOP COMPUTERS AT THE BORDER

While many courts have grappled with what level of suspicion, if any, is required for a laptop border search to be constitutional, most have found that the search at issue was supported by reasonable suspicion, and, thus, did not discuss or decide whether searches of laptop computers could occur without probable cause or reasonable suspicion, generally speaking. For instance, in *United States v. Irving*,⁷² the Second Circuit held that the search of the defendant's computer diskettes and undeveloped film was supported by reasonable suspicion, and, thus, the court did not "determine whether [these searches] were routine or non-routine."⁷³ While many courts have stopped their analysis after finding reasonable suspicion, a few courts have dealt with the issue of laptop border searches more directly.

A. *United States v. Ickes*

In *United States v. Ickes*,⁷⁴ the Fourth Circuit affirmed a denial of the defendant's motion to suppress evidence found during a border search.⁷⁵ Ickes was entering the United States from Canada at a port of entry near Detroit, Michigan.⁷⁶ The U.S. Customs inspector was "puzzled" when Ickes told him that he was returning from vacation because his "van appeared to contain 'everything he owned.'"⁷⁷ After finding marijuana and photographs of young boys in the van, agents placed Ickes under arrest and continued searching the van—they seized a computer and seventy-five disks, which contained additional child pornography.⁷⁸

Ickes urged the court to recognize a First Amendment exception to the border search doctrine, which is, itself, an exception to the Fourth Amendment.⁷⁹ He claimed that the border search exception did not apply to "expressive material,"

72. 452 F.3d 110 (2d Cir. 2006).

73. *Id.* at 124. The lower court in *United States v. Irving*, 2003 U.S. Dist. LEXIS 16111, at *15 (S.D.N.Y. Sept. 15, 2003), had stated in dicta that the search of the diskettes and undeveloped film may have been constitutional even without reasonable suspicion. *See also* Jared Spitalnick, Comment, *United States v. Irving (decided September 15, 2003)*, 49 N.Y.L. SCH. L. REV. 425, 425 (2004) (arguing that this "dicta could provide the basis for a troubling expansion of the border-search doctrine").

74. 393 F.3d 501 (4th Cir. 2005).

75. *Id.* at 502.

76. *Id.*

77. *Id.*

78. *Id.* at 503.

79. *Id.* at 505-06. Ickes also claimed that the search of his computer and disk did not fall within the statutory language of 19 U.S.C. § 1581(a) (2000), through which Congress has authorized border searches. *Ickes*, 393 F.3d at 504. However, due to the sweeping language of the statute and the history of the government's power to conduct routine searches at the border, the court dismissed this argument quickly. *Id.* at 503-05.

and that the court's ruling was sweeping and could lead to the search of every laptop on any international flight.⁸⁰ Ickes did not argue that the laptop search was too invasive of his privacy rights, thus constituting a violation of the Fourth Amendment itself.

The court refused to create a First Amendment exception to the border search doctrine.⁸¹ In so doing, the court's language seemed to extend even beyond rejecting the First Amendment exception argument. The court emphasized the government's strong "overriding interest in securing the safety of its citizens" as it applies to border searches generally.⁸² The court said that this interest must be balanced against "a lesser interest on the side of the potential entrant," whose "expectation of privacy [while not at his or her home] is substantially lessened."⁸³ The court also expressed its concern with the implementation of a First Amendment exception, stating that this "would ensure significant headaches for those forced to determine its scope These sorts of legal wrangles at the border are exactly what the Supreme Court wished to avoid by sanctioning expansive border searches."⁸⁴

The defendant in this case was unsympathetic to be sure. However, the court's ruling was broader than necessary. The court could have denied the defendant's motion solely on the basis of the finding that the search of the computer and disks was based on a reasonable suspicion, and, thus, constitutional. Albums of nude boys in the van had already been found.

In rejecting Ickes' argument that the court's ruling was overly sweeping, the court stated, "[a]s a practical matter, computer searches are most likely to occur where—as here—the traveler's conduct or the presence of other items in his possession suggest the need to search further"; in other words, when there is reasonable suspicion.⁸⁵ By so stating, the court implied that it identifies border searches solely as a matter of practicality and is not willing to extend legal protection to travelers, *requiring* reasonable suspicion for these searches. The court did not address whether laptop computer searches are routine or not, but by implication, the court seemed to assume that they are routine.

The court in *Ickes* also characterized the traveler's interest very narrowly: "Since 'a port of entry is not a traveler's home,' his expectation of privacy there is substantially lessened."⁸⁶ This reasoning begs the question of what the traveler's expectation of privacy really is under the circumstances. The court focused on the traveler's expectation of privacy at the border generally, while it should have focused, instead, on the privacy interest at stake here—the expectation of privacy in the computer and disks specifically.

80. *Ickes*, 393 F.3d at 506-07.

81. *Id.* at 507.

82. *Id.* at 506.

83. *Id.*

84. *Id.*

85. *Id.* at 507 (emphasis added).

86. *Id.* at 506 (quoting *United States v. Thirty-Seven Photographs*, 402 U.S. 363, 376 (1971)).

While the court's language in *Ickes* was very broad, the bottom line of the court's reasoning was fairly narrow; the court rejected the defendant's arguments that the search at hand was unconstitutional and affirmed the conviction. The defendant's main argument was that the court should carve out a First Amendment exception to the border search doctrine.⁸⁷ It is the defendant's argument that was a large part of the problem, leading to the sweeping dicta. For one, the exception argued for was very broad. Indeed, part of the reason the court rejected it is because it would "create a sanctuary at the border for all expressive material—even for terrorist plans."⁸⁸ Secondly, the Supreme Court in an earlier case had rejected a First Amendment exception for warrant applications, thus the Fourth Circuit in *Ickes* stated: "Given the Court's reluctance to create a First Amendment exception to the general principles governing warrant applications, we find it unlikely that it would favor a similar exception to the border search doctrine."⁸⁹

A different argument, one based on the Fourth Amendment and the strong privacy interests of the traveler, may have been more successful. Further, any rule formulated in this area of the law must take into account the nation's countervailing security interests, and thus should allow for laptop searches if there is reason to believe the person is a threat to our nation's security. Perhaps this is why the court rejected the First Amendment argument so strongly.

B. *United States v. Romm*

In the summer of 2006, the Ninth Circuit decided a laptop border search case that garnered much attention.⁹⁰ In *United States v. Romm*,⁹¹ the court denied a motion to suppress images of child pornography and affirmed the defendant's convictions.⁹² The defendant, Romm, had flown from Las Vegas, where he was attending a training seminar, to Kelowna, British Columbia.⁹³ Canada's Border Services Agency stopped Romm for questioning after discovering that Romm had a criminal history.⁹⁴ An agent examined Romm's laptop and saw several child pornography websites in the laptop's "internet history."⁹⁵ Upon further questioning, Romm admitted that this was in violation of the terms of his

87. *Id.*

88. *Id.*

89. *Id.* at 507.

90. See, e.g., Seidenberg, *supra* note 13; Declan McCullagh, *Police Blotter: Laptop Border Searches OK'd*, CNET NEWS.COM, July 26, 2006, http://news.com.com/2100-1030_3-6098939.html; NewsTarget, *Homeland Security Can Now Search Your Laptop Computer: Man Gets 25 Years for Deleted Image Files*, NEWSTARGET.COM, July 27, 2006, <http://www.newstarget.com/019790.html>.

91. 455 F.3d 990 (9th Cir. 2006), *cert. denied*, 127 S. Ct. 1024 (2007).

92. *Id.* at 1006.

93. *Id.* at 994.

94. *Id.*

95. *Id.*

probation.⁹⁶ Canada's immigration service decided not to allow Romm entrance into the country, and Romm took the next flight out to Seattle.⁹⁷ At the Seattle-Tacoma airport, Romm was interviewed by U.S. Customs officials, who informed him that they needed to search his laptop.⁹⁸ Romm agreed, and a forensic analysis of the hard drive was performed.⁹⁹ The analysis revealed ten pictures of child pornography, all of which had been deleted.¹⁰⁰

"Romm was convicted of knowingly receiving and knowingly possessing child pornography in violation of" federal law and received "concurrent mandatory minimum sentences of ten and fifteen years."¹⁰¹ Romm appealed the conviction, setting forth numerous arguments. He argued, most importantly, that the search of the laptop intruded on his First Amendment rights and was, therefore, not a routine border search.¹⁰² The court declined to consider this issue because it was not raised by the defense in its opening brief and was, thus, "deemed waived."¹⁰³ The Court noted the *Irving* and *Ickes* cases, as well as the Supreme Court case of *Flores-Montano*, in a footnote and stated that they were not deciding "whether the search of Romm's laptop was 'non-routine,' and if so, whether it was supported by reasonable suspicion."¹⁰⁴ Apparently, the defense did not make a Fourth Amendment argument. Thus, these issues were left open for future cases to decide.

C. United States v. Arnold

In *United States v. Arnold*,¹⁰⁵ the United States District Court for the Central District of California decided one of the issues that went unaddressed by the Ninth Circuit in *Romm*. The court granted a motion to suppress evidence found during a border search of the defendant's laptop, CDs, and memory stick.¹⁰⁶ The defendant, Arnold, had arrived at Los Angeles International Airport after a long flight from the Philippines.¹⁰⁷ Arnold was selected for secondary questioning by

96. *Id.*

97. *Id.*

98. *Id.*

99. *Id.*

100. *Id.* at 994-95.

101. *Id.* at 993.

102. *Id.* at 997. Romm set forth several other arguments with regards to the border search exception, arguments that were specific to the facts of his case. For instance, Romm argued that he had "never *legally* crossed the U.S.-Canada border," and thus could not be subjected to a border search. *Id.* at 996. The court stated that there was no support for this proposition, and that the issue was whether the traveler "*physically* crossed the border." *Id.*

103. *Id.* at 997.

104. *Id.* at 997 n.11.

105. 454 F. Supp. 2d 999 (C.D. Cal. 2006).

106. *Id.* at 1001.

107. *Id.*

a customs officer.¹⁰⁸ The officer turned Arnold's laptop on to see if it was working, and after the computer booted up, two officers viewed the pictures saved in two Kodak files.¹⁰⁹ After finding a picture of two nude women, one of the officers called in special agents, who found child pornography saved on the laptop.¹¹⁰

The court noted that "the oft-quoted phrase 'searches made at the border . . . are reasonable simply by virtue of the fact that they occur at the border' belies the fact that highly intrusive searches are not reasonable merely because they take place at the border."¹¹¹ The court held that a search of a computer's hard drive or other electronic storage devices implicates the privacy and dignity interests of a person.¹¹² The court stated that the search of the contents of a laptop or electronic storage device was more intrusive than the search of "a lunchbox or other tangible object."¹¹³

While the court realized that a laptop search is not physically intrusive, it stated that it "can be just as much, if not more, of an intrusion into the dignity and privacy interests of a person. This is because electronic storage devices function as an extension of our own memory."¹¹⁴ The court held that since these interests were implicated, a laptop search is a non-routine search, requiring reasonable suspicion and limited scope.¹¹⁵ Because the court found that the search in this case was not supported by reasonable suspicion, the motion to suppress the evidence was granted.¹¹⁶

This case is the first to recognize that laptop searches implicate privacy and dignity interests. Further, it is the first to clearly hold that a laptop border search is "non-routine." This case has since been appealed to the Ninth Circuit.¹¹⁷

108. *Id.*

109. *Id.*

110. *Id.*

111. *Id.* at 1002 (quoting *United States v. Flores-Montano*, 541 U.S. 149, 152-53 (2004)).

112. *Id.* at 1003.

113. *Id.*

114. *Id.* at 1000.

115. *Id.* at 1002-04.

116. *Id.* at 1007.

117. As Professor Orin Kerr stated: "The interesting question is whether the Ninth Circuit will agree," and "[i]f the Ninth Circuit does agree with Judge Pregerson that computer searches are 'non routine,' there's a decent chance that this case would be the first computer search and seizure case to get to the Supreme Court." Posting of Orin Kerr to *The Volokh Conspiracy*, <http://volokh.com/posts/1160582029.shtml> (Oct. 11, 2006, 11:53 EST); *see also* Matt Krasnowski, *LAX Laptop Search Heads for Appeal on Privacy Issue*, DAILYBREEZE.COM, Nov. 11, 2006, <http://www.dailybreeze.com/news/articles/4618646.html?page=1&c=y> (quoting Shaun Martin, a professor at the University of San Diego School of Law, to have said: "There's no doubt in my mind that the Supreme Court will review one of these cases The issue is too important and it happens too often to let the results vary depending on what border you happen to cross or what circuit you're in.").

III. THE SEARCH OF A LAPTOP COMPUTER AT THE BORDER IS NOT A ROUTINE BORDER SEARCH

A. *The Search of a Laptop Computer at the Border Is Inconsistent with the Rationale Behind the Border Search Exception*

Anytime the Court establishes a new exception to the warrant and probable cause requirements, it delineates the reasons it is doing so. Often there are important policy reasons supporting the category of warrantless searches at hand.¹¹⁸ Sometimes the Court finds that the policies supporting the warrant requirement are not implicated in the category of searches at issue, and, thus, does away with the warrant requirement for those searches.¹¹⁹ With regards to border searches, the Court has justified it as follows: “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.”¹²⁰ Put another way, the Court has stated that Congress has given “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.”¹²¹ This is based in part on “Congress[’s] broad . . . powers ‘to regulate Commerce with foreign Nations.’ Historically such broad powers have been necessary to prevent smuggling and to prevent prohibited articles from entry.”¹²²

Because all of the reasons justifying the border search doctrine are usually framed in terms of “who and what may enter the country,”¹²³ these justifications do not apply to suspicionless laptop border searches. The information saved on a laptop can be transported into our country electronically, regardless of whether the traveler or the laptop crosses the border. For instance, in *Romm*, the defendant had accessed the photos from child pornography websites.¹²⁴ These

118. See, e.g., *Terry v. Ohio*, 392 U.S. 1, 24 (1968) (upholding a “stop” and “frisk” based on reasonable suspicion because “we cannot blind ourselves to the need for law enforcement officers to protect themselves and other prospective victims of violence in situations where they may lack probable cause for an arrest”).

119. See, e.g., *Colorado v. Bertine*, 479 U.S. 367, 371 (1987) (quoting *South Dakota v. Opperman*, 428 U.S. 364, 370 n.5 (1976)) (upholding the constitutionality of warrantless inventory searches because “[t]he policies behind the warrant requirement are not implicated in an inventory search, nor is the related concept of probable cause: ‘The standard of probable cause is peculiarly related to criminal investigations, not routine, noncriminal procedures.’” (citation omitted)).

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

121. *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985).

122. *Id.* at 537-38 (citing *United States v. Ramsey*, 431 U.S. 606, 618-19 (1977)) (citation omitted).

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

124. *United States v. Romm*, 455 F.3d 990, 994 (9th Cir. 2006), *cert. denied*, 127 S. Ct. 1024 (2007).

websites could have been accessed anywhere in the world. Even if the defendant had not downloaded the photos onto his laptop and transported them into this country, others living in our country could have accessed the same websites and downloaded the photos without even coming close to our international border. In other words, the presence of the pornography on the laptop was incidental to the border crossing.

Further, law enforcement efforts would not be frustrated by requiring reasonable suspicion as they would be in other contexts; officers could have caught Romm with the pornography inside the country, even if he had crossed the border without being detected. This is in direct contrast with a drug dealer, who is likely to sell the drugs for cash upon crossing the border, never to be caught or prosecuted for his crimes.¹²⁵

While catching people who violate pornography laws is an important government interest, general crime or terrorism prevention is not the justification behind the border search exception. In *Colorado v. Bertine*,¹²⁶ the Court upheld the constitutionality of inventory searches because they are conducted for non-criminal purposes.¹²⁷ The Court emphasized that if a search is done “solely for the purpose of investigating criminal conduct,” its validity is “dependent on the application of the probable-cause and warrant requirements of the Fourth Amendment.”¹²⁸ Thus, intrusive border searches may not be conducted solely for the purpose of catching criminals or terrorists; rather, they must be consistent with the traditional rationales justifying the border search—the prevention of the entry of illegal aliens and contraband into our country.

In *Terry v. Ohio*, the Court upheld the constitutionality of a “stop” and “frisk” based merely on reasonable suspicion because of the strong interest in protecting police and other third parties.¹²⁹ The Court made it clear, however, that the scope of the search must be consistent with the justifications supporting the exception in the first place: “The sole justification of the search . . . is the protection of the police officer and others nearby, and it must therefore be confined in scope to an intrusion reasonably designed to discover guns, knives, clubs, or other hidden instruments for the assault of the police officer.”¹³⁰

Likewise, the scope of a routine border search must be consistent with the justification for the border search. The scope of the intrusion must be “reasonably designed” to prevent entry of illegal aliens and contraband. Thus, for the purpose of preventing entry of illegal aliens, U.S. Customs officials can check a traveler’s passport and Customs Border Patrol declaration, and address any issues arising from these documents.¹³¹ Consistent with the rationale of

125. Comment, *Intrusive Border Searches—Is Judicial Control Desirable?*, 115 U. PA. L. REV. 276, 283-84 (1966).

126. 479 U.S. 367 (1987).

127. *Id.* at 371.

128. *Id.* (emphasis added).

129. 392 U.S. 1, 29 (1968).

130. *Id.*

131. U.S. CUSTOMS AND BORDER PROTECTION, A LOOK AT THE CBP TRAVELER INSPECTION

preventing entry of contraband, officials may x-ray and search a traveler's car, luggage, and any goods he or she may have.¹³² They may also conduct a personal search, which includes a search of the outer clothing, purse, wallet, or pockets.¹³³ A traveler may be asked to take a laptop computer out of carry-on bags and let it pass through scanners so that border officials may "get an unimpeded look at each computer . . . help[ing] them discern whether it contains hidden explosives" or other illegal substances.¹³⁴ To ensure that a laptop is not hiding a weapon or contraband, the laptop may also be opened by officials.¹³⁵ Finally, laptop officials may turn the laptop computer on to ensure that it is functioning normally.¹³⁶ All of these examinations of a laptop are quick, relatively limited intrusions, and, most importantly, consistent with the rationale of the border search doctrine—preventing the entry of illegal aliens and goods. However, clicking on the various icons of the laptop computer to view photos and read various documents falls outside the scope of this rationale. Suspicionless laptop border searches are not necessary for our government to prevent the entry of illegal aliens and contraband. Child pornography or other illegal photos will still enter into our country, regardless of these suspicionless searches, due to the nature of the Internet and electronic communications.

In *Ickes*, the Fourth Circuit recognized that "[t]he border search doctrine is justified by the 'longstanding right of the sovereign to protect itself,'" but went on to say: "Particularly in today's world, [where] national security interests may require uncovering terrorist communications . . ." ¹³⁷ While the government has a strong interest in uncovering terrorist communications, this should not be enough to justify suspicionless laptop border searches of all travelers. Rather, by requiring reasonable suspicion, a standard lower than probable cause, the courts will allow the government to continue with its important job of investigating potential terrorists, while, still, protecting travelers' privacy interests.

PROCESS (2006), <http://www.customs.ustreas.gov/linkhandler/cgov/toolbox/publications/travel/whyexamc.ctt/whyexamc.pdf>.

132. LAFAVE, *supra* note 5, § 10.5(a).

133. *Id.*

134. Daniel Engber, *What Makes Laptops So Dangerous?: Why They Get Special Attention at the Airport*, SLATE, Nov. 22, 2005, <http://www.slate.com/id/2130910/>. As a result of this common practice of asking travelers to remove their laptops from carry-on bags, many travelers have been forgetting or losing their laptops at airports. See, e.g., Chris Woodyard, *Fliers Lose Laptops at Airport Checkpoints*, USA TODAY, Feb. 19, 2002, at 1A, available at <http://www.usatoday.com/money/biztravel/2002-02-20-lost-laptops.htm>. As the Author of this Note recently witnessed while traveling through Denver International Airport, this has prompted the posting of "Got laptop?" signs, which appear shortly after proceeding through security checkpoints, in at least one airport. See also *id.*

135. Engber, *supra* note 134.

136. *Id.*

137. *United States v. Ickes*, 393 F.3d 501, 506 (4th Cir. 2005) (citing *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004) (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977))).

As a general matter, it is important for courts to take into account changed circumstances when formulating new laws or dealing with new cases. In a post-September 11 world, we have increased national security interests. The Supreme Court took into account changed circumstances and current events in *Montoya de Hernandez*, when it recognized that there was a “national crisis in law enforcement caused by smuggling of illicit narcotics,” and that smugglers were increasingly using deceptive practices, including the “utilization of alimentary canal smuggling.”¹³⁸

What distinguishes the consideration of current events in *Montoya de Hernandez* from the use of recent events in *Ickes*, however, is that in *Montoya de Hernandez*, the “crisis,” namely the increase in smuggling of drugs, was consistent with the traditional rationale for the border search doctrine—preventing the entry of contraband into this country.¹³⁹ In *Ickes*, however, the language was more sweeping than any of the traditional rationales for the border search doctrine, since “uncovering terrorist communications” may involve more than the usual routine border search.

*B. The Search of a Laptop Computer at the Border Is More than
“a Relatively Limited Invasion”*

The search of a laptop at the border is more than “a relatively limited invasion.” As noted, it is only when a search is a “relatively limited invasion” that the *Camara* balancing test justifies a border search merely on the basis that a person has crossed the border.¹⁴⁰ If the invasion is “more intrusive, there is a need to strike the balance [between the need to search and the invasion which the search entails] anew.”¹⁴¹ More intrusive searches are not considered to be routine searches and require some level of suspicion to be constitutional.¹⁴²

1. *The Search of a Laptop at the Border Implicates Travelers’ Strong Privacy Interests.*—In *Flores-Montano*, the Court pointed to the interests that may “support a requirement of some level of suspicion”—the “dignity and privacy interests of the person being searched.”¹⁴³ Most courts have taken these interests into account as they have considered the question of what constitutes a non-routine search in other contexts. All of these courts, however, have focused on physical intrusion.¹⁴⁴ This may be because those cases consistently arose in

138. *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985) (citation omitted).

139. *Id.* at 537-38.

140. LAFAVE, *supra* note 5, § 10.5(a).

141. *Id.* § 10.5(c).

142. *See id.* (discussing the level of suspicion, at least reasonable suspicion, required for strip searches to be constitutional).

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

144. *See, e.g., United States v. Braks*, 842 F.2d 509, 512 (1st Cir. 1988) (setting forth six factors to be considered when determining the degree of invasiveness of a search: “(i) whether the search results in the exposure of intimate body parts or requires the suspect to disrobe; (ii) whether physical contact between Customs officials and the suspect occurs during the search; (iii) whether

the context of intrusive physical searches. Thus, the approaches taken in those cases cannot readily be applied to the laptop search cases at hand.

While *Arnold* was the first case to find a traveler's privacy interests implicated in a laptop search, this may be because the trend of carrying laptops while traveling has only recently become widespread. Indeed, *Arnold* was one of the first few cases to have dealt with this issue at all. Nonetheless, taking into account the various uses of the laptop computer, as well as the strong reliance many travelers have come to have on their laptops, one can reach the same conclusion. In an article expressing concern over the recent laptop border search cases and the idea that government officials could search her laptop without any suspicion or a warrant, one legal commentator stated:

My laptop computer was purchased by Stanford, but my whole life is stored on it. I have e-mail dating back several years, my address book with the names of everyone I know, notes and musings for various work and personal projects, financial records, passwords to my blog, my web mail, project and information management data for various organizations I belong to, photos of my niece and nephew and my pets.

In short, my computer is my most private possession. I have other things that are more dear, but no one item could tell you more about me than this machine.¹⁴⁵

This commentator lists some of the things one may have stored on his or her laptop—family pictures, financial records, and passwords to email are just a few examples. This illustrates how private computers can be. Furthermore, she emphasizes that “no one item could tell you more about me than this machine.”¹⁴⁶ Indeed, a laptop search could reveal just as much private information about a person as a strip search or other intrusive body search can, albeit of a different kind.

Before the advent of the laptop computer, it is unlikely that one would travel carrying all of his or her intimate letters, confidential financial information, and all of his or her family albums. However, the laptop has changed the way people do things. Since this information can easily be stored electronically, people have replaced paper versions of records with electronic ones, and store them on their laptops and take them along for convenience purposes. Thus, while papers are sometimes searched during a routine border search,¹⁴⁷ a laptop search is very different. One can easily control which papers he or she carries in a purse or pocket, but it is not possible to do the same when it comes to a laptop, which may

force is used to effect the search; (iv) whether the type of search exposes the suspect to pain or danger; (v) the overall manner in which the search is conducted; and (vi) whether the suspect's reasonable expectations of privacy, if any, are abrogated by the search” (footnotes omitted)).

145. Jennifer Granick, Commentary, *Computer Privacy in Distress*, WIRED, Jan. 17, 2007, <http://www.wired.com/politics/law/commentary/circuitcourt/2007/01/72510>.

146. *Id.*

147. *See, e.g.,* United States v. Fortna, 796 F.2d 724, 738 (5th Cir. 1986).

contain an immense amount of information.

While routine border searches may be conducted without any level of suspicion, the courts have drawn the line at more intrusive body searches, such as strip searches, requiring a showing of “reasonable” suspicion.¹⁴⁸ Laptop border searches should be on the same side of the line as these intrusive body searches. Laptops may contain private photographs of the traveler and his or her family. Those photographed may have been scantily dressed and posing in a manner that they would not present themselves in public. Thus, the laptop search may be an intrusion into the traveler’s privacy and bodily integrity. Further, the search of the hundreds or thousands of files saved on a laptop is time-consuming; thus, a traveler who is pulled over for an extended period of time may feel stigmatized and embarrassed.

The courts have not been ambivalent to how private computers, in general, can be. In numerous other contexts, courts have recognized that people have a reasonable expectation of privacy in their computers and afforded this expectation Fourth Amendment protection.¹⁴⁹ In a recent Ninth Circuit case, *United States v. Ziegler*,¹⁵⁰ the court held that the private employees have a reasonable expectation of privacy in their workplace computers.¹⁵¹ The court based its holding in part on a previous U.S. Supreme Court case, which held that private employees have a reasonable expectation of privacy in their workplaces, even if the office was shared by several employees.¹⁵² Further, the court stated that the defendant had a reasonable expectation of privacy based on the facts in this case; the defendant did not share his office with his co-workers, and he also kept it locked.¹⁵³

Ziegler demonstrates that the court was willing to recognize that ““for most people, their computers are their most private spaces,”” thus leading to a recognition of a legitimate expectation of privacy in the computer.¹⁵⁴ This reasoning should be given greater weight in the laptop computer situations because laptop computers are more private than workplace computers—workplace computers are unlikely to contain family photographs, personal diaries, or private financial information. Also, a laptop computer is usually not shared by others, and the data is sometimes “locked,” or protected by a password or encryption. Similar facts were noted by the court in *Ziegler* as providing further support for the defendant’s expectation of privacy.¹⁵⁵ Thus,

148. See HUBBART, *supra* note 59, at 288.

149. See generally Robin Cheryl Miller, Annotation, *Validity of Search or Seizure of Computer, Computer Disk, or Computer Peripheral Equipment*, 84 A.L.R.5th 1 (2000).

150. 474 F.3d 1184 (9th Cir. 2007).

151. *Id.* at 1190.

152. *Id.* at 1189 (citing *Mancusi v. DeForte*, 392 U.S. 364 (1968)).

153. *Id.* at 1190.

154. *Id.* at 1189 (quoting *United States v. Gourde*, 440 F.3d 1065, 1077 (9th Cir. 2006) (en banc) (Kleinfeld, J., dissenting)).

155. *Id.* at 1190 (noting that the defendant did not share his office with co-workers and kept it locked).

just as private employees have a legitimate expectation of privacy in their workplace computers, travelers have a legitimate expectation of privacy in their laptop computers and should be provided with Fourth Amendment protection—it should be unconstitutional for border officials to search the contents of a laptop without, at the least, reasonable suspicion.

Another point illustrated by *Ziegler* is that cases involving computers and other technologies raise a similar dilemma—the courts must base their holdings on prior precedents, which did not involve technology. In *Ziegler*, the court drew the analogy between an office and the computer in the office.¹⁵⁶ It was not hard to see the similarity between the two contexts because the computer is in the office. It may be harder to find a parallel to laptop computers. One can think of the laptop as a closed container, which, as a general matter, may be searched during a routine border search.¹⁵⁷ By defining a laptop in this manner, however, one would be limiting the scope of the search of a laptop to the scope of the search of a closed container, namely opening it and looking inside for illegal substances. This is the kind of laptop search officials routinely conduct—opening the laptop, making sure it does not have contraband hidden inside, and turning the laptop on to ensure it is working properly.¹⁵⁸ The files saved on a laptop's hard drive, however, differ markedly from the physical contents of a closed container, and thus this analogy seems incomplete.

Another analogy that can be drawn is between intrusive physical searches, which require suspicion, and laptop searches. While the body and laptop computers are very different, a person's laptop computer resembles his or her memory, as noted by the court in *Arnold*:

While not physically intrusive as in the case of a strip or body cavity search, the search of one's private and valuable personal information stored on a hard drive . . . can be just as much, if not more, of an intrusion into the dignity and privacy interests of a person. *This is because electronic storage devices function as an extension of our own memory.*¹⁵⁹

It may be necessary for the lower courts to draw this analogy, so that existing precedents will work and apply to the new laptop computer cases. Or the courts may simply recognize that technology has had a great impact on this area of the law, and declare that travelers have a legitimate expectation of privacy in their laptop computers. This would create a consistency between modern technologies, travelers' expectations, and the law in this area.

156. *See id.*

157. *See, e.g.,* Henderson v. United States, 390 F.2d 805, 808 (9th Cir. 1967) (stating that a “person crossing our border may be required to disclose the contents of his baggage, and of his vehicle” and “[w]e assume that the same rule would apply to the contents of his or her purse, wallet, or pockets”).

158. *See supra* notes 134-36 and accompanying text.

159. United States v. Arnold, 454 F. Supp. 2d 999, 1000 (C.D. Cal. 2006) (emphasis added).

2. *Travelers' Privacy Interests in Their Laptops Outweigh the Government's Need to Conduct Suspicionless Laptop Searches at the Border.*—To determine whether a search is reasonable, a balance must be made between the government's need to conduct the search at hand and the privacy interests at stake.¹⁶⁰ In the case of laptop computer border searches, travelers' privacy interests in their laptops outweigh the government's need to conduct suspicionless laptop searches.

In *United States v. Place*,¹⁶¹ the Supreme Court held that a detention of a piece of luggage for ninety-minutes had "exceeded the bounds of a permissible investigative detention of the luggage."¹⁶² The defendant in *Place* aroused the suspicions of law enforcement officers as he stood in line at Miami International Airport to buy a ticket to La Guardia Airport in New York.¹⁶³ When the defendant arrived in New York, he found two DEA agents waiting for him.¹⁶⁴ After refusing to consent to the search of his luggage, the agents seized his luggage and took it to Kennedy Airport, where a "sniff test" was conducted on the bags and a narcotics detection dog reacted positively to one of the two bags.¹⁶⁵ Ninety minutes had passed since the luggage was first seized.¹⁶⁶

While the search and seizure at issue in *Place* took place in an airport, they were not conducted as part of an airport or border search. Rather, the Court applied the principles from *Terry v. Ohio*, which allows for a "stop" and "frisk" as long as it is supported by reasonable suspicion.¹⁶⁷ The Court stated, however, that while *Terry* allows for investigative stops based on reasonable suspicion, this does not end the inquiry; "[w]e must balance 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."¹⁶⁸ As a part of this balancing, the Court recognized that there are degrees of intrusiveness, and while "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 specific articulable facts that the property contains contraband or evidence of a crime,"¹⁶⁹ in this case, "[t]he length of the detention of respondent's luggage alone precludes the conclusion that the seizure was reasonable in the absence of probable cause."¹⁷⁰ The Court, therefore, held that the detention at issue was unconstitutional.¹⁷¹

160. See *Camara v. Municipal Court of S.F.*, 387 U.S. 523, 533-34 (1967).

161. 462 U.S. 696 (1983).

162. *Id.* at 698.

163. *Id.*

164. *Id.*

165. *Id.* at 699.

166. *Id.*

167. *Id.* at 702 (citing *Terry v. Ohio*, 392 U.S. 1 (1968)).

168. *Id.* at 703.

169. *Id.* at 706.

170. *Id.* at 709.

171. *Id.* at 709-10.

In the case of laptop border searches, strong privacy interests of travelers are implicated. Travelers have an interest in protecting personal items saved on their laptops, such as diaries, personal financial information, and passwords, which may be characterized as an “extension of our own memory.”¹⁷² Business professionals and attorneys also have an interest in protecting the privacy of client information they have saved on the laptop, which they are under a duty to do.

On the other hand is the government’s need to conduct suspicionless searches of laptops—to open any laptop it would like and spend time clicking on the various icons, reading files, and looking at photos. While a border official opening a laptop, ensuring it does not have drugs or weapons, and turning it on may be acting within the scope of the Constitution, as were the police when they initially detained the defendant in *Place*, the extended time and degree of the intrusion should render the laptop border search unconstitutional, as it did in *Place*.

IV. LESSONS FROM *KYLLO* AND *KATZ*: NEW TECHNOLOGIES OFTEN WARRANT NEW RULES

While the constitutionality of laptop border searches is a relatively new issue that the courts must deal with, this is not the first time a new technology has affected Fourth Amendment jurisprudence. In *Kyllo v. United States*,¹⁷³ the Supreme Court grappled with the question of whether “a thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within the home constitutes a ‘search’ within the meaning of the Fourth Amendment.”¹⁷⁴ In *Kyllo*, the scan of the defendant’s house with the thermal-imaging device revealed to agents that portions of the house “were relatively hot.”¹⁷⁵ The agents concluded that the defendant “was using halide lights to grow marijuana in [the] house.”¹⁷⁶ Eventually, a search warrant was issued and over 100 marijuana plants were found.¹⁷⁷ The defendant “was indicted on one count of manufacturing marijuana.”¹⁷⁸

The *Kyllo* Court expressed a concern that new technologies may diminish our privacy: “The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.”¹⁷⁹ The Court held, in an opinion by Justice Scalia, that “[w]here, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the

172. *United States v. Arnold*, 454 F. Supp. 2d 999, 1000 (C.D. Cal. 2006).

173. *Kyllo v. United States*, 533 U.S. 27 (2001).

174. *Id.* at 29.

175. *Id.* at 30.

176. *Id.*

177. *Id.*

178. *Id.*

179. *Id.* at 34.

surveillance is a ‘search’ and is presumptively unreasonable without a warrant.”¹⁸⁰

In *Katz v. United States*,¹⁸¹ a much earlier case, the Supreme Court also dealt with a new technology and how it would impact our Fourth Amendment rights. In *Katz*, the Court held that government officials listening in through an electronic listening and recording device fastened to the outside of a telephone booth were in violation of the Fourth Amendment.¹⁸² The Court was, once again, well-aware of the impact technology had on our expectations of privacy. The Court noted:

One who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. *To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.*¹⁸³

The set of circumstances in *Kyllo* and *Katz* were very different from what we have here when confronting the issue of laptop border searches; yet, the concern is the same—will the new technologies and the new set of circumstances that arise as a result of these technologies diminish our right to privacy? In *Kyllo*, the new technology at issue, the thermal-imaging device, was used to actually conduct the surveillance.¹⁸⁴ This differs markedly from what we have in the laptop cases, where those being subjected to the search are the ones utilizing the technology. In *Katz*, the technology, the electronic recording device, was used to eavesdrop on the defendant by government officials, but the defendant himself was also using a technology—the telephone booth.¹⁸⁵ Thus, regardless of how the technology is used, the issue is the same; as Justice Scalia put it: “The question we confront . . . is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.”¹⁸⁶

In both *Kyllo* and *Katz*, the Court recognized the changes technology has made to our lives and formed a rule that protected our right to privacy. The same is necessary here—a rule that recognizes that travelers’ expectation of privacy in the contents of their laptops is akin to the privacy interest they have in their bodies and their homes, all of which require some level of suspicion before a search is conducted by government officials.

180. *Id.* at 40.

181. 389 U.S. 347 (1967).

182. *Id.* at 359.

183. *Id.* at 352 (emphasis added).

184. *Kyllo*, 533 U.S. at 29.

185. *Katz*, 389 U.S. at 348.

186. *Kyllo*, 533 U.S. at 34.

V. PRACTICAL IMPLICATIONS: SHOULD TRAVELERS LEAVE THEIR LAPTOPS AT HOME WHEN TRAVELING ABROAD?

Until a clear rule comes out of these cases, travelers need to realize that the content of their laptops may be searched when crossing our country's border regardless of who they are or how they act. If a traveler does not want to be subjected to such a search, he or she may be better off leaving his or her laptop at home. Attorneys or other professionals who have confidential information on their laptops may have a duty to do so from here on out.¹⁸⁷ Even if the confidential information is not downloaded or saved to the laptop itself, if that information has been recently accessed, the laptop may have created temporary files of the information, which can be recovered through forensic examination.¹⁸⁸ Deleted images or files can also be recovered by forensic analysis.¹⁸⁹

It is not clear what would happen if the information on the laptop is encrypted or protected by a password,¹⁹⁰ thus, “[p]erhaps the only way to guarantee protection for confidential data is to leave your laptop at home and connect to your data via a computer that stays overseas.”¹⁹¹ This will inevitably result in changes to the way businesses and firms conduct their business.¹⁹²

CONCLUSION

The courts should hold that for a search of the content of a traveler's laptop at the border to be constitutional, it must be based on, at the least, reasonable

187. See MODEL RULES OF PROF'L CONDUCT R. 1.6 (2003) (“A lawyer shall not reveal information relating to the representation of a client.”); see also Seidenberg, *supra* note 13.

188. Seidenberg, *supra* note 13.

189. See *United States v. Romm*, 455 F.3d 990, 995 (9th Cir. 2006), *cert. denied*, 127 S. Ct. 1024 (2007). In *Romm*, even though the defendant had deleted all of the child pornography he had viewed on his laptop, government officials were able to recover these files through forensic analysis. *Id.* Analysis can also reveal when the files or images were “created, accessed, or modified.” *Id.*

190. See A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 829 (1995) (arguing that “a properly guarded key to a cryptographic system” is an “item of information for which the user would have both a subjectively and objectively reasonable expectation of privacy” and thus should be given Fourth Amendment protection); *but cf.* Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a “Reasonable Expectation of Privacy?”*, 33 CONN. L. REV. 503, 505 (2001) (“argu[ing] that encryption cannot create Fourth Amendment protection”). It is to be noted that this on-going debate between scholars is not in the context of the border search doctrine.

191. Seidenberg, *supra* note 13.

192. See James Gilden, *Laptop Seizure Raises Concerns over Firms' Data: Travel Managers Worry About What Can Happen to Proprietary Information at Customs*, L.A. TIMES, Nov. 4, 2006, at C4 (reporting that “[e]ighty-six percent of members [of the Association of Corporate Travel Executives, an Alexandria, Virginia-based trade group] surveyed said that court decisions allowing government agents to seize computers at the borders were cause to limit the kind of proprietary information typically carried on executives' laptops”).

suspicion. This will be consistent with travelers' expectation of privacy, and will not lead to an unwarranted expansion of the border search doctrine.¹⁹³ While all of the cases that have arisen so far have involved defendants caught with pornography and prosecuted for their crimes, the courts should take a step back and consider how their rulings will affect us all because the rules "'fashion[ed] [are] for the innocent and guilty alike.'"¹⁹⁴

The government has a strong interest in protecting the integrity of the border and ensuring that illegal aliens and contraband do not enter our country. However, this interest is not as strong in the case of laptop computer border searches because the material saved on a laptop computer may enter our nation regardless of the laptop or the border crossing. The government also has a very strong interest in preventing terrorism; yet, this must be kept within the confines of a reasonable suspicion standard to protect the majority of travelers, most of whom are innocent of any terrorist activities.

Many travelers have come to rely heavily on their laptops. During the long airplane rides, they may work on their laptops to pass the time. If traveling for business purposes, the laptop may have important documents and files, essential to the conduction of business. Most hotels provide Internet access for their guests, allowing them to use the laptop in the hotel room for work, school, or communicating with loved ones back home. If the courts do not take these changed circumstances into account, travelers may have to choose between their laptop and their expectation of privacy and desire to avoid the embarrassment and hassles of a laptop border search. Justice Brennan, many years ago, in *Montoya de Hernandez*, issued a warning of what may occur if we were to take the safeguards provided to us by our Constitution lightly:

[I]f there is one enduring lesson in the long struggle to balance individual rights against society's need to defend itself against lawlessness, it is that "[it] is easy to make light of insistence on scrupulous regard for the safeguards of civil liberties when invoked on behalf of the unworthy. It is too easy. History bears testimony that by such disregard are the rights of liberty extinguished, heedlessly at first, then stealthily, and brazenly in the end."¹⁹⁵

Many years have passed since Justice Brennan warned against "mak[ing] light of insistence on scrupulous regard for the safeguards of civil liberties,"¹⁹⁶ however, in light of modern technology and current events, we need to take his warning more seriously than ever before.

193. See also Spitalnick, *supra* note 73, at 425.

194. *Illinois v. Gates*, 462 U.S. 213, 290 (1983) (Brennan, J., dissenting) (quoting *Draper v. United States*, 358 U.S. 307, 314 (1959) (Douglas, J., dissenting)).

195. *United States v. Montoya de Hernandez*, 473 U.S. 531, 567 (1985) (Brennan, J., dissenting) (quoting *Davis v. United States*, 328 U.S. 582, 597 (1946) (Frankfurter, J., dissenting)).

196. *Id.*