Washington Journal of Law, Technology & Arts

Volume 5 | Issue 2 Article 4

10-1-2008

Border Searches of Laptop Computers after *United States v. Arnold*: Implications for Traveling Professionals

Cooper Offenbecher

Corporate & Commercial
Cite as: Cooper Offenbecher, *Border Searches of Laptop Computers after United States v. Arnold: Implications for Traveling Professionals*, 5 SHIDLER J. L. Com. & Tech. 9 (2008), *available at* <http://www.lctjournal.washington.edu/vol5/a09Offenbecher.html>

BORDER SEARCHES OF LAPTOP COMPUTERS AFTER UNITED STATES V. ARNOLD: IMPLICATIONS FOR TRAVELING PROFESSIONALS

Cooper Offenbecher[1]

Abstract

The Ninth Circuit Court of Appeals recently held that border searches of laptop computers do not require reasonable suspicion. The decision, in *United States v. Arnold*, reflects the continued intent of the Ninth Circuit—along with the Fourth Circuit Court of Appeals—to continue analyzing laptop computer searches under the traditional border search doctrine. This article will examine recent laptop computer search cases in light of the border search doctrine and will consider the implications for lawyers and business professionals who travel abroad with confidential information on laptops and other electronic-storage devices. The article will also consider the implications of such searches on the ethical duty of confidentiality, the attorney-client privilege, and trade secrets law.

Table of Contents

INTRODUCTION

<1>As our society becomes increasingly globalized, technology continues to develop smaller, more powerful computerized devices. As our penchant for carrying information on and communicating via such devices increases, lawyers and business professionals find

themselves carrying vital information all around the world. Whether it be a laptop computer; a memory stick; a personal digital assistant (PDA); a Blackberry, iPhone, or other "smartphone"; or a conventional cellular phone, electronic devices continue to increase in popularity as they allow individuals to conduct business from almost anywhere. Recent cases involving border searches of laptop computers have raised questions concerning the privacy of information carried on electronic devices. Under the traditional border search doctrine, when individuals enter the country, officials do not need a reason to search the individuals or their belongings. However, with the continuing advances in technology, the issue becomes whether the border search doctrine extends to information contained on personal computerized and electronic devices, and what happens when such information is found during a search.

<2>The Ninth Circuit Court of Appeals recently held in *United States v. Arnold* that border searches of laptop computers do not require reasonable suspicion.[2] The Fourth Circuit Court of Appeals—the other circuit to have definitively decided this issue—also has held that such searches do not require reasonable suspicion.[3] Other courts have similarly upheld searches of laptop computers by customs officials as falling within the traditional border search doctrine.[4] This article considers the evolution of the border search doctrine and carefully examines its application to the cases involving searches of laptop computers. The article then considers the potential impact of such searches on the ethical duty of confidentiality, the attorney-client privilege, and the abandonment of trade secrets doctrine. Ultimately, the article concludes that an increase in laptop searches combined with courts currently allowing such searches should cause professionals traveling internationally to take note.

THE BORDER SEARCH DOCTRINE: ROUTINE VS. NON-ROUTINE SEARCHES

<3>Border searches of persons entering the United States have long been considered permissible.[5] The United States Supreme Court has consistently held that the Fourth Amendment's protection against unreasonable searches and seizures is qualitatively different at the border because of the nation's security interests;[6] protecting our borders is essential to the nation's health, safety, and welfare.[7] As a result, "routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant."[8]

<4>Courts have struggled to define what constitutes a "routine" search and what constitutes a "non-routine" search. In *Montoya de Hernandez*, the Court suggested in a footnote that border searches such as strip, body cavity, or involuntary x-ray searches might be considered "non-routine" and therefore require a different level of

suspicion than other border searches.[9] The Ninth Circuit Court of Appeals has noted that the degree of intrusiveness is one of the most important factors in determining whether a search is routine or non-routine.[10] In *United States v. Ramos-Saenz*, the Ninth Circuit held that a border search becomes non-routine "only when it reaches the degree of intrusiveness present in a strip search or body cavity search."[11]

<5>The border search doctrine has been extended to include the examination of luggage and other containers by x-ray or other technological means.[12] In *United States v. Okafor*, after an x-ray examination, customs officials emptied the defendant's suitcase as he was entering the country at Los Angeles International Airport.[13] Suspecting a hidden compartment, the officials inserted a needle probe into the luggage and detected cocaine.[14] The Supreme Court upheld the completed x-ray as a routine search, holding that such an examination may be done at the border without any showing of particularized suspicion "so long as the means of examination are not personally intrusive, do not significantly harm the objects scrutinized, and do not unduly delay transit."[15] The court explained that border searches become non-routine only when they reach the level of invasiveness of a strip search or body cavity search.[16] The court, however, did not need to decide whether the search was routine or non-routine since the court held that the officers had reasonable suspicion.

<6>The Supreme Court has consistently upheld quite intrusive searches as within the scope of the border search doctrine. In *United States v. Flores-Montano*, for example, the Supreme Court held that a defendant who entered the country by car did not have a privacy interest in the car's fuel tank, and therefore the complete disassembly of the fuel tank did not require reasonable suspicion.[17] The court stated that the inquiry of whether a search was "routine" or "non-routine simply did not apply to searches of vehicles.[18] As a result, the court limited the inquiry concerning whether a search was routine to situations involving searches of a person and his or her personal effects. However, the court seemingly left open the question of whether or not a "particularly offensive" search, or one with exceptional property damage, might require a heightened level of suspicion.[19]

THE DOCTRINE EXTENDED: LAPTOP COMPUTERS

<7>Recently, courts have had to decide how to apply the border search doctrine to searches of laptop computers. This section will consider the earlier cases on border searches of laptops and a subsequent section will discuss the *Arnold* case. In *United States v. Ickes*, the United States Court of Appeals for the Fourth Circuit held

that electronic files contained on disks and a computer found in the defendant's van constituted "cargo" within the meaning of a federal statute authorizing searches.[20] There, the defendant was attempting to enter the United States from Canada at a border crossing when officials searched his van and found incriminating material, including images of child pornography on his laptop and disks.[21]

<8>In *Ickes*, the court upheld the statutory authority of customs officials under the Tariff Act.[22] The court explained that Congress had been emphatic in its empowerment of customs officials to search vehicles entering the country:

> Any officer of the customs may at any time go on board of any vessel or vehicle at any place in the United States or within the customs waters, . . . or at any other authorized place . . . and examine the manifest and other documents and papers and examine, inspect, and search the vessel or vehicle and every part thereof and any person, trunk, package, or cargo on board.[23]

<9>The court rejected the defendant's contention that the term "cargo" did not encompass the computer and the disks and noted that "to hold otherwise would undermine the longstanding practice of seizing goods at the border even when the type of good is not specified in the statute."[24] Further, the court held that the search was reasonable simply because it occurred at the border.[25] The court did not mention the distinction between routine and non-routine border searches. In addition, the court stated that the border search doctrine was not subject to a First Amendment exception.[26] The court explained that given the reluctance of courts to allow First Amendment exceptions to warrant applications, it declined to create such an exception for border searches.[27]

<10>Shortly after *Ickes*, the Ninth Circuit Court of Appeals considered the issue of a border search of a laptop computer. In *United States v. Romm*, the Ninth Circuit Court of Appeals upheld, as routine, the search of the defendant's laptop computer at an airport upon entry to the United States.[28] Because the petitioner had raised the issue for the first time in his reply brief, the court declined to answer the question of whether the search was non-routine and therefore entitled to heightened scrutiny.[29] However, in a footnote, the court commented that the Supreme Court's decision in *Flores-Montano* "suggests that the search of a traveler's property at the border will always be deemed 'routine,' absent a showing the search technique risks damage to the searched property."[30] *Romm* seems to suggest that all laptop searches will be permissible as long as the search does not risk damaging the computer.

<11>In another recent case, *United States v. Irving*, the Second Circuit Court of Appeals upheld a border search of computer disks when reasonable suspicion was present. The court declined to decide whether the search was routine or non-routine because there was reasonable suspicion for the search.[31] In *Irving*, the customs officials had information suggesting that the defendant had traveled abroad to engage in illegal activities.[32] A subsequent search turned up floppy disks containing child pornography.[33] The court examined the information the officials had about the defendant and his travels and determined that the customs officials had a reasonable basis for examining the disks. Therefore, the court did not need to inquire into whether the search was routine or non-routine.[34] The court, however, suggested that absent reasonable suspicion a court would have to determine whether the search was routine or non-routine.[35]

THE NINTH CIRCUIT'S DECISION IN UNITED STATES V. ARNOLD

<12>In April 2008, the Ninth Circuit joined the Fourth Circuit and held that a border search of a laptop computer did not require reasonable suspicion.[36] The decision is particularly important because it reversed a district court decision that had held reasonable suspicion was required for border searches of laptop computers.[37] In *United States v. Arnold*, the defendant was charged with several counts related to possession of child pornography.[38] While waiting in the customs line at Los Angeles International Airport, the defendant was selected for secondary questioning.[39] After questioning, Customs and Border Patrol officers searched his luggage and obtained a laptop computer, a separate hard drive, a flash drive, and six compact discs.[40] An examination of these items revealed images depicting what the officers believed to be child pornography.[41] The district court granted the defendant's motion to suppress, finding that the officers needed reasonable suspicion to search the laptop and that the government did not have reasonable suspicion in this particular case.[42] After noting that non-routine, invasive border searches require reasonable suspicion, the court found that "the search of a computer hard drive and similar electronic storage devices implicates privacy and dignity interests of a person."[43] The court stated that "[p]eople keep all types of personal information on computers, including diaries, personal letters, medical information, photos and financial records. Attorneys' computers may contain confidential client information. Reporters' computers may contain information about confidential sources or story leads. Inventors' and corporate executives' computers may contain trade secrets."[44] Because the search of a laptop was similar to more invasive searches of the person, the court held that reasonable suspicion

was required to search a laptop.[45]

<13>The Ninth Circuit Court of Appeals, however, reversed the district court's decision.[46] The appellate court stated that courts have long recognized that border searches of closed containers can be done without reasonable suspicion.[47] Specifically, the court noted cases where searches of briefcases, purses, wallets, pockets, papers found in pockets, pictures, films, and other graphic materials were all held permissible even absent reasonable suspicion.[48] The court went on to explain that the Supreme Court has only limited the border search power when intrusive searches of *the person* occur, or in certain situations involving the destruction of property.[49] It rejected the district court's reliance on cases involving searches of the person, stating that the application of a sliding intrusiveness scale to a case involving the search of property is simply misplaced.[50] Distinguishing from searches of persons, the court essentially rejected the distinction between routine and non-routine searches, stating that the terms are merely descriptive and are inapplicable to searches involving property.[51] As a result, the court held that "reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border."[52]

<14>The Court of Appeals went further than merely rejecting the reasoning used by the district court. Perhaps in an effort to show that it had considered other potential arguments, the Ninth Circuit addressed additional exceptions and challenges to the border search rule that had not been discussed by the district court. The Court of Appeals noted that *Flores-Montano* left open two possible narrow grounds upon which reasonable suspicion might be required.[53] The first exception not addressed in *Flores-Montano* is whether "exceptional damage to property" occurred.[54] However, the *Arnold* court declined to consider this issue because the defendant in *Arnold* had never raised the issue. The second potential exception is whether the search was particularly offensive.[55] The *Arnold* court explained that the defendant failed to show how the search of his laptop was logically different from other traditional border searches of luggage that the Supreme Court has repeatedly allowed;[56] the defendant's comparison of a laptop search to the search of a home was without merit because the Supreme Court has rejected applying heightened Fourth Amendment protection to property simply because it has privacy interests similar to those associated with a home.[57] Furthermore, the court stated that in other situations courts have refused to find searches "particularly offensive" simply because, as is the case with electronic storage devices, the container has an increased storage capacity.[58] Finally, the court adopted the reasoning of the Fourth Circuit in *Ickes* and refused to create a First Amendment exception to the border search

doctrine.[59]

WHEN CAN LAPTOP COMPUTERS BE SEARCHED?

<15>While the cases discussed above involve child pornographic imagery, the more important issue for traveling businesspersons and lawyers is whether or not these decisions give customs officials the right to search and seize information *other* than child pornography. These cases do not distinguish between child pornography and other types of information (i.e., attorney-client privileged information, company strategies, or business trade secrets). Indeed, there have been recent cases in which international business travelers have had their laptop computers seized and searched.[60] Travelers and advocacy organizations have become increasingly worried about electronic searches and several organizations have filed lawsuits concerning this matter.[61] However, because searches of businesspersons and lawyers have not generally resulted in criminal prosecutions, there are no published cases addressing border searches of laptops in those situations. Thus, the consideration of the border search doctrine as applied to traveling professionals takes place in the context of the published cases involving child pornography.

<16>Currently, the law provides that laptop computers can be searched by customs officials without any reasonable suspicion. After *Romm*, there was hope that laptop searches might still be subject to an inquiry into whether the search was routine or non-routine. In *Arnold*, just three years later, the Ninth Circuit rejected the application of the routine and non-routine distinction to searches involving laptop computers.[62] There, the Ninth Circuit was considering a district court opinion that, if upheld, would have changed the face of the border search doctrine by requiring reasonable suspicion for laptop searches.[63] Perhaps as a result, the court takes the time to address, not only the district court's reasoning, but also the *Flores-Montano* exceptions to the First Amendment argument.[64] By rejecting the possibility that a laptop search, by its intrusive nature, could be a non-routine search requiring heightened scrutiny, *Arnold* refuses to apply the standard involved in searches of persons to those of electronic storage devices.[65]

<17>Further, while *Ickes* deals more narrowly with a statute authorizing searches of vehicles and vessels entering the country,[66] the Fourth Circuit's interpretation likely gives officials carte blanche to search everything in the vehicle—including confidential documents. By rejecting the First Amendment challenge to the search, the Fourth Circuit may have foreclosed all constitutional avenues of attack. As this article will later discuss, other doctrines such as the attorney-client privilege and the ethical

duty of confidentiality may likely restrict how information obtained during a search may be used. However, *Ickes* and *Arnold* show that challenges to the inherent power to make the search may be futile. As a result, the current state of the law suggests that customs agents may search ordinary travelers' laptop computers without probable cause, a warrant, or reasonable suspicion, and obtain admissible evidence that may be used against the traveler in later litigation.

<18>The *Irving* case, while facially different than the above cases, offers insight into how the courts will apply the border search doctrine. In *Irving*, the Second Circuit skirted the inquiry into whether or not the search was routine or non-routine by finding reasonable suspicion based on information the customs officials had concerning the defendant. However, as discussed above, reasonable suspicion is not needed for border searches; customs officials can search individuals and their property absent any articulable reason. Further, as with all reasonable suspicion inquiries, the court retroactively applied the analysis after the officials had found the incriminating evidence. As a result, the *Irving* court may have paved the way for other courts to avoid inquiring into whether the border search was routine by identifying limited facts sufficient to constitute reasonable suspicion.

THE ETHICAL DUTY OF CONFIDENTIALITY FOR LAWYERS TRAVELING ABROAD

<19>It is important to consider the duty of confidentiality to understand whether lawyers violate the ethical rules of professional conduct when traveling through customs checkpoints with laptops and other electronic devices that contain confidential client information. The ethical duty of confidentiality is one of the hallmarks of the legal profession and the attorney-client relationship. Model Rule of Professional Conduct ("MRPC") 1.6(a) states that "[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted . . . ."[67] Because client confidences might be exposed during a border search of a laptop, it is important to know if such disclosure constitutes an ethical violation.

<20>Based on the text and comments of the MRPC, it seems unlikely that courts or other disciplinary tribunals would find that a lawyer violated the ethical duty of confidentiality simply by traveling through border checkpoints with confidential client information on his or her laptop computer. The comments to the MRPC state that a lawyer must act competently to safeguard information relating to the representation of a client against disclosure.[68] Competent representation is defined by the MRPC as "the legal knowledge,

skill, thoroughness and preparation reasonably necessary for the representation."[69] The MRPC comments further explain that

> When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions.[70]

<21>As discussed above, the information is at risk of being seen and read by border officials who have the apparent right to open laptop computers and look at the information contained within. Traveling through customs checkpoints with client confidences on a laptop is not affirmative disclosure under MRPC 1.6(a) and does not violate the explicit prohibition against revealing information. In addition, the risk of "inadvertent or unauthorized disclosure" is low, and traveling with client confidences in an electronic format is a widespread practice among lawyers.[71] Finally, the practice among many professionals to password protect computer access and other information would likely be considered a reasonable precaution against disclosure under the MRPC.

<22>If the exposure of confidential communications during a border search is analogized to the interception of email communications, lawyers likely would not violate their ethical duty by traveling with such information. In 1999, the American Bar Association (ABA) issued an ethics opinion stating that a lawyer may transmit information relating to the representation of a client by means of unencrypted email without violating the Model Rules of Professional Conduct.[72] The opinion noted that the "mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint."[73] Most states have adopted positions similar to that of the ABA.[74] If a similar analysis was applied to border searches of laptops, lawyers would not violate their ethical duty of confidentiality by traveling with confidential information, even if that information was exposed during a search.

<23>However, some states have taken a different stance than the ABA regarding attorney-client communications.[75] For example, two states have cautioned attorneys to seek client consent or inform clients of the risks before communicating via email.[76] Other states have even advised against communicating sensitive client information by way of email.[77] If courts or disciplinary tribunals were to apply these standards to the border search situation, they could find that attorneys had violated the ethical duty of confidentiality by traveling through border checkpoints with

confidential information on laptop computers.

WAIVER OF THE ATTORNEY-CLIENT PRIVILEGE AND TRAVELING LAWYERS

<24>The inadvertent disclosure of information during a border search also raises the question of whether such a disclosure constitutes a waiver of the attorney-client privilege. The attorney-client privilege protects certain types of communications between attorneys and clients. The policy behind the privilege is that such information should be inadmissible at trial in order to encourage full and frank communication between attorneys and their clients.[78] The privilege is an evidentiary doctrine that is governed by the common law[79] and protects communications between attorneys and clients unless the protection is waived.[80]

<25>When considering inadvertent disclosure of privileged information during discovery, courts have generally taken three approaches to determine when and whether the attorney-client privilege has been waived.[81] Under the lenient approach, disclosure of client confidences generally does not create a waiver of the privilege.[82] Under the middle-of-the-road approach, courts employ a multi-faceted reasonableness test in determining whether the privilege has been waived.[83] These courts have considered factors such as the reasonableness of precaution taken to prevent disclosure, number of inadvertent disclosures, extent of the disclosures, promptness of measures taken to rectify the disclosure, and "whether the overriding interest of justice would be served by relieving the party of its error."[84] Finally, under the strict approach, disclosure is the equivalent of waiving the attorney-client privilege: "[I]f a client wishes to preserve the privilege, it must treat the confidentiality of attorney-client communications like jewels-if not crown jewels. Short of court-compelled disclosure, or other equally extraordinary circumstances, we will not distinguish between various degrees of 'voluntariness' in waivers of the attorney-client privilege."[85]

<26>If we apply the principles used in the context of inadvertent disclosure during discovery, it seems unlikely that courts would hold that disclosure of privileged information, by way of a border search, constitutes waiver of the attorney-client privilege. However, the existence of the privilege depends upon which approach a court uses. Courts employing the lenient approach likely would not find such a disclosure had waived the privilege because those courts are more likely to forgive disclosures without finding a waiver of privilege. Courts using the middle-of-the-road approach also likely would not find that the privilege had been waived because traveling with privileged information in compact computerized devices is commonplace and widely accepted. These middle-of-the-road approach courts likely would find that such travel does not

constitute a failure to take reasonable precautions against disclosure, particularly if the disclosure is a single instance. However, some courts could interpret "reasonable precautions" differently. For example, as mentioned in the previous section, some jurisdictions require consent prior to communicating by email or advise against sending sensitive client information over email at all. Courts in these jurisdictions might define "reasonable precautions" in a more exacting manner. These courts may find that "reasonable precautions" require affirmative action, such as protecting client communications with a complicated password system or by storing the information on a home server to be accessed once the attorney was abroad.

<27>Similar to the middle-of-the-road approach, under the strict approach, it is also unclear whether or not disclosure during a border search would constitute a waiver. Courts using the strict approach could determine that attorneys traveling the world with privileged information on computerized devices—in light of the fact that such information can be examined at will by customs officials—have waived the privilege by failing to take adequate precautions and failing to treat their clients' information as "crown jewels." Another possibility is that these courts could find that disclosure by way of a border search is equivalent to court compelled disclosure or equally extraordinary circumstances. Thus, such action could also be found to not constitute a waiver under even the strict approach to attorney-client privilege waiver.[86] Consequently, whether or not a court would find that disclosure during a border search constitutes a waiver of the attorney-client privilege depends on which approach to privilege waiver the court takes, as well as possibly the jurisdiction's general acceptance of electronic communications.

TRAVELING PROFESSIONALS AND THE POSSIBLE ABANDONMENT OF TRADE SECRETS

<28>International business travelers who travel with proprietary information on electronic storage devices may be concerned about the disclosure of trade secrets to customs and border patrol agents. However, disclosure during a border search is unlikely to cause trade secrets to lose their protected status. American courts generally create a cause of action for the disclosure or misuse of trade secrets by persons who obtain knowledge of the secret in certain circumstances.[87] General public disclosure of a trade secret results in abandonment that can cause the secret to lose its protected status and preclude parties from recovering for the disclosure or misuse of the secret.[88] However, situations with a limited disclosure may not result in abandonment.[89] Courts have also held that disclosure of trade secrets to public officials does not result in abandonment.[90]

<29>The disclosure of trade secrets to customs or border agents as

a result of a border search of a laptop computer or other electronic storage device is unlikely to constitute abandonment such that the trade secrets would lose their protected status.[91] First, the compelled disclosure of trade secrets resulting from a border search of a laptop computer is not a public disclosure. Second, the disclosure of trade secrets to a few agents is likely to be considered a limited disclosure; the information is viewed by a select group of individuals who are conducting the search, and, as noted above, limited disclosures of trade secrets may not result in abandonment. Finally, Customs and Border Patrol agents are probably considered "public officials." In *Plastic & Metal Fabricators, Inc.*, the court held that mere "inspection by a public official does not contradict the element of secrecy."[92] Consequently, the disclosure of trade secrets resulting from a border search of a laptop computer is unlikely to constitute the abandonment of a trade secret.

CONCLUSION

<30>The Ninth Circuit and the Fourth Circuit have affirmatively held that border searches of laptop computers and other electronic storage devices do not require reasonable suspicion. Under the current cases, information acquired by customs officials during such searches is admissible in litigation as fruit of a permissible border search. However, if the information is by nature an attorney-client communication, a claim of attorney-client privilege is likely to succeed. Further, it is unlikely that those who travel internationally with electronically stored information are violating the ethical duty of confidentiality or are abandoning trade secrets. While the reported cases in this area of law deal with child pornography, nothing in the decisions limits the scope of the border search doctrine or restricts officials from searching other types of information. While laptop searches are rare, traveling professionals have been targeted as well. Though the risk is low, lawyers and business professionals who travel abroad with confidential and privileged information run the risk that customs officials will read the electronic information.

<< Top

Footnotes

1. Cooper Offenbecher, University of Washington School of Law, J.D. program Class of 2008. Thank you to Professor Jane Winn of the University of Washington School of Law, Laura Dunlop, student editor, and Professor Orin Kerr of the George Washington University Law School for reviewing this article.

2. United States v. Arnold, 523 F.3d 941, 946 (9th Cir. 2008).

3. United States v. Ickes, 393 F.3d 501 (4th Cir. 2005).
4. *See* United States v. Romm, 455 F.3d 990 (9th Cir. 2006); United States v. Irving, 452 F.3d 110 (2d Cir. 2006); United States v. Ickes, 393 F.3d 501 (4th Cir. 2005).
5. United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985).
6. United States v. Ramsey, 431 U.S. 606, 616 (1977).
7. United States v. Okafor, 285 F.3d 842, 845 (2002).
8. *Montoya de Hernandez*, 473 U.S. at 538.
9. *Montoya de Hernandez*, 473 U.S. at 541 n.4.
10. United States v. Sandoval Vargas, 854 F.2d 1132, 1134 (9th Cir. 1988), *abrogated by* United States v. Taghizadeh, 41 F.3d 1263 (9th Cir. 1994).
11. United States v. Ramos-Saenz, 36 F.3d 59, 61 (9th Cir. 1994).
12. *Okafor*, 285 F.3d at 844.
13. *Id*.
14. *Id.*
15. *Id.* at 846. Because of an insufficient record, the court declined to decide whether the needle incision constituted a non-routine search, but hinted that if the suitcase had been significantly damaged, that would tend to make the search non-routine. *Id*. n.1.
16. *Id.*
17. United States v. Flores-Montano, 541 U.S. 149, 149 (2004) ("Respondent's assertion that he has a privacy interest in his fuel tank, and that the suspicionless disassembly of his tank is an invasion of his privacy, is rejected, as the privacy expectation is less at the border than it is in the interior, and this Court has long recognized that automobiles seeking entry into this country may be searched." (citation omitted)).
18. *Flores-Montano*, 541 U.S. at 149 ("The reasons that might support a suspicion requirement in the case of highly intrusive searches of persons simply do not carry over to vehicles.").
19. *Id.* at 154, 154 n.2.
20. United States v. Ickes, 393 F.3d 501 (4th Cir. 2005).

21. *Id.* at 502-03.

22. *Id.* at 503-04.

23. *Id.* (citing 19 U.S.C. § 1581(a) (2000)).

24. *Ickes*, 393 F.3d at 505.

25. *Id.*

26. *Id.*

27. *Id.*

28. *Romm*, 455 F.3d at 997.

29. *Id*.

30. *Id.* at 997 n.11.

31. United States v. Irving, 452 F.3d 110, 124 (2d Cir. 2006).

32. *Id.*

33. *Id.*

34. *Id.*

35. *Id*.

36. United States v. Arnold, 523 F.3d 941, 946 (9th Cir. 2008).

37. *Id.* at 948.

38. *Id.* at 943.

39. United States v. Arnold, 454 F. Supp. 2d 999, 1001 (C.D. Cal. 2006), *rev'd*, 523 F.3d at 946.

40. *Id.*

41. *Id.*

42. *Id.* at 1007.

43. *Id.* at 1003.

44. *Id.* at 1003-04.

45. *Id.* at 1004.

46. United States v. Arnold, 523 F.3d 941, 948 (9th Cir. 2008).

47. *Id.* at 945.

48. *Id.* (citing United States v. Tsai, 282 F.3d 690, 696 (9th Cir. 2002) (traveler's briefcase and luggage); Henderson v. United States, 390 F.2d 805, 808 (9th Cir. 1967)

(traveler's purse, wallet, or pockets); United States v. Grayson, 597 F.2d 1225, 1228-29 (9th Cir. 1979) (papers found in traveler's shirt pocket); United States v. Thirty-Seven Photographs, 402 U.S. 363, 376 (1971) (pictures, films and other graphic materials)).

49. United States v. Arnold, 523 F.3d 941, 945 (9th Cir. 2008) (citing *Flores-Montano*, 541 U.S. at 152).

50. *Id.* at 945-46.

51. *Id.* at 946 (citing United States v. Cortez-Rocha, 394 F.3d 1115, 1123 (9th Cir. 2005); *Flores-Montano*, 541 U.S. at 152; United States v. Chaudhry, 424 F.3d 1051, 1054 (9th Cir. 2005)).

52. *Id.* at 946.

53. *Id.* (citing *Flores-Montano*, 541 U.S. at 155-56).

54. *Id.* at 946-47.

55. *Id.*

56. *Id.* at 947.

57. In rejecting the argument, the court explained (1) that one cannot live in a laptop, and that (2) the defendant himself readily admits that a laptop goes with the person, and is "readily mobile." *Id*. (citing California v. Carney, 471 U.S. 386, 393-94 (1985)) (rejecting the argument that a mobile home should be afforded the same level of protection as an actual home, simply because it was "capable of functioning as a home").

58. *Id.* at 947 (citing California v. Acevedo, 500 U.S. 565, 576 (1991) (rejecting that the search of a closed container within a car is unreasonable, when officials were already properly searching a car)).

59. United States v. Arnold, 523 F.3d 941, 948 (9th Cir. 2008) (citing *Ickes*, 393 F.3d at 502).

60. Cathleen O'Connor Schoultz, Another Business Travel Concern: Laptops Being Seized at Border, Association Warns, Ass'n of Corporate Travel Executives, June 19, 2007, https://www.acte.org/resources/press_release.php?id=177.

61. *See* Kelly Fiveash, *EFF and Chums Sue Feds over Border Laptop Inspections*, The Register, Feb. 8, 2008, http://www.theregister.co.uk/2008/02/08/eff_alc_sues_homeland_secur ; Ellen Nakashima, *Clarity Sought on Electronic Searches*, The Washington Post, Feb. 7, 2008, A01,

available at http://www.washingtonpost.com/wp-dyn/content/article/2008/02/06/AR2008020604763.html.

62. *Arnold*, 523 F.3d at 945-46.

63. *Id.*

64. *Id.* at 946-47.

65. *Id.* at 945-46.

66. United States v. Ickes, 393 F.3d 501, 503-04 (4th Cir. 2005).

67. Model Rules of Prof'l Conduct R. 1.6(a) (2004).

68. Model Rules of Prof'l Conduct R. 1.6 cmt. 16 (2004).

69. Model Rules of Prof'l Conduct R. 1.1 (2004).

70. Model Rules of Prof'l Conduct R. 1.6 cmt. 17.

71. Andrew Beckerman-Rodau, *Ethical Risks from the Use of Technology*, 31 Rutgers Computer & Tech. L.J. 1, 25 (2004).

72. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999).

73. *Id.*

74. *Id.* at n.40.

75. *See id.*

76. *See* Pa. Bar Ass'n Comm. on Legal Ethics, Op. 97-130 (1997); State Bar of Ariz. Advisory, Op. 97-04 (1996).

77. *See* Iowa Bar Ass'n, Op. 1997-1 (1997); N.C. State Bar, Op. 215 (1995).

78. Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

79. *See, e.g.*, Fed. R. Evid. 501.

80. 8 J. Wigmore, Evidence § 2292 554 (McNaughton rev. 1961).

81. Gray v. Bicknell, 86 F.3d 1472, 1483 (1996).

82. *Id.*

83. *Id.*

84. Hartman v. El Paso Natural Gas Co., 763 P.2d 1144, 1152 (1988)(N.M 1988).

85. In re Sealed Case, 877 F.2d 976, 980 (D.C. Cir. 1989) (citation omitted).

86. *Id.*

87. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 (1995).

88. *See*, *e.g.*, Wilkes v. Pioneer Am. Ins. Co., 383 F. Supp. 1135, 1140-41 (D.S.C. 1974); Underwater Storage, Inc. v. U.S. Rubber Co., 371 F.2d 950, 955 (1966).

89. *See*, *e.g.*, Philadelphia Extracting Co. v. Keystone Extracting Co., 176 F. 830, 831 (1910); *Wilkes*, 383 F. Supp. at 1140.

90. *See*, *e.g.*, *Wilkes*, 383 F. Supp. at 1141 (holding that the originator of method had right to rely on limited degree of confidentially in dealings with government officials in official capacity); Plastic & Metal Fabricators, Inc. v. Roy, 163 Conn. 257, 269 (1972) (stating that "inspection by a public official does not contradict the element of secrecy.").

91. This article limits the discussion of trade secrets to the narrow issue of whether the compelled disclosure of trade secrets as a result of a border search constitutes abandonment. A separate, much broader and involved issue is simply whether the disclosure or misuse of the trade secrets by the customs and border agents constitutes a breach of traditional trade secrets law. That particular issue is beyond the scope of this article.

92. *Plastic & Metal Fabricators, Inc.*, 163 Conn. at 269.