NEW YORK LAW SCHOOL

NYLS Law Review

Volume 49
Issue 1 *State of Play*

Article 17

January 2004

United States v. Irving

Jared Spitalnick
New York Law School

UNITED STATES V. IRVING
(decided September 15, 2003)

JARED SPITALNICK*

With the advanced storage capacities available on modern computer hard drives, should a customs agent have the authority to freely search a traveler's computer files simply because the traveler is crossing a border, or does this authority infringe on a traveler's right to privacy? In *United States v. Irving*,[1] the United States District Court for the Southern District of New York held that a United States customs agent can go as far as developing film and viewing the contents of computer files when "reasonable suspicion"[2] is present.[3] However, in dicta, the *Irving* court further opined that a customs agent may inspect the contents of computer files regardless of whether "reasonable suspicion" is present or not.[4] This is significant because, according to the court, a customs agent can pull aside a traveler with a computer and freely search each individual file on the computer without any justification. A customs agent could also read sensitive personal information or confidential corporate or legal documents simply because the computer passes through a border. This case comment will argue that while the *Irving* holding was correct, the court's dicta could provide the basis for a troubling expansion of the border-search doctrine.[5] In doing so, this case comment will first examine why the search of computer files should be considered "non-routine,"[6] and therefore requires a "reasonable

* J.D. Candidate, 2005, New York Law School.

1. 2003 WL 22127913 (S.D.N.Y. 2003).

2. United States v. Rivas, 157 F.3d 364, 367 (5th Cir. 1998) ("'Reasonable suspicion is defined as 'a particularized and objective basis for suspecting the particular person' of smuggling contraband.'") (citation omitted).

3. *Irving*, 2003 WL 22127913, at *5.

4. *Id.*

5. The border-search doctrine states that searches conducted at international borders do not require a warrant, probable cause, or any suspicion to justify the search, as long as the search is "routine" – i.e. – it does not "seriously invade a traveler's privacy." Rivas, 157 F.3d at 367 (5th Cir. 1993), *citing* United States v. Cardenas, 9 F.3d 1139, 1147 (5th Cir. 1993).

6. See discussion *supra* note 5.

suspicion" standard. This case comment will next analyze the problem of classifying a computer as a "closed container" for the purposes of a Fourth Amendment search. It will then examine the holdings of *United States v. Molina-Tarazon*[7] and *United States v. Soto-Teran*[8] to argue that without a "reasonable suspicion" standard, the search of computer files could lead to psychological apprehension and an impermissible invasion of privacy.

In 1982, Stefan Irving pled guilty to a charge of first degree sexual assault.[9] In 1996, the government initiated a nationwide investigation aimed at preventing suspected pedophiles from traveling to Mexico to engage in sexual acts with children.[10] Two years later, Irving became a subject of the government's nationwide investigation.[11]

On May 27, 1998, Irving was traveling back to the United States from Mexico when he was stopped and searched by customs agents at the Dallas-Fort Worth Airport.[12] No pornography or evidence of a crime was found during the search.[13] However, Irving was in possession of children's books and what appeared to be children's drawings.[14] Customs agents then questioned Irving,[15] and he admitted to being a convicted pedophile.[16] The agents went through Irving's luggage and found children's drawings, several children's books, a disposable camera, and two computer diskettes.[17] The agents developed the film and checked the content on the diskettes.[18] Subsequently, the film proved to contain no pornography but the diskettes revealed some evidence of child erotica.[19]

7. 279 F.3d. 709, 713 (9th Cir. 2000).
8. 44 F. Supp. 2d. 185 (E.D.N.Y. 1996).
9. *Irving*, 2003 WL 22127913, at *1.
10. *Id.*
11. *Id.*
12. *Id.*
13. *Id.*
14. *Id.*
15. *Irving*, 2003 WL 22127913, at *1.
16. *Id.*
17. *Id.*
18. *Id.* at *2.
19. *Id.*; *see also* United States v. Hudak, 2003 WL 22170606, at *1 (S.D.N.Y. 2003) (defining "child erotica" as "images of nude children that do not rise to the level of pornography").

Irving was later charged with traveling abroad with the intent to have sex with children, and receipt and possession of child pornography.[20] Irving moved to suppress the statements he made and the evidence seized by the customs agents on May 27, 1998.[21] Irving argued that the search was not "routine,"[22] but was part of the government's investigation of travelers suspected of going to Mexico to commit sexual acts on children.[23]

The district court denied the motion to suppress the evidence seized on May 27, 1998.[24] The court found that customs agents had reasonable suspicion for their search and that the motive in initiating the search was immaterial in the border context.[25] The court stated that customs officials had a reasonable basis for suspecting that Irving's camera, film, and computer diskettes contained pornographic images.[26] First, the customs agents knew Irving was a convicted pedophile.[27] Second, Irving was carrying children's books and drawings, and was returning from an orphanage in Mexico.[28] Finally, Irving was a subject of the government's ongoing investigation of individuals suspected of traveling to Mexico to engage in sexual acts with children.[29] Regardless of this finding, the court stated in dictum that, "the agents were entitled to inspect the contents of the [computer] diskettes even absent reasonable suspicion."[30] The court based this statement on the notion that a computer is a "closed container,"[31] and therefore comes within the scope of a routine border search.[32]

---

20. *Irving*, 2003 WL 22127913, at *1.

21. *Id.* This case comment will only address the search and not the issue regarding the statements Irving made to the customs agents.

22. *See supra* note 5.

23. *Irving*, 2003 WL 22127913, at *4.

24. *Id.* at *6.

25. *Id.* at *4-5.

26. *Id.* at *5.

27. *Id.*

28. *Id.* at *5.

29. *Irving*, 2003 WL 22127913, at *1.

30. *Id.* at *5.

31. *See* McCormick v. City of Lawrence, 289 F.Supp.2d 1264, 1266 (D. Kan. 2003) (comparing a personal computer to a closed container under a Fourth Amendment analysis).

32. *Irving*, 2003 WL 22127913, at *5.

The court's decision in *Irving* should be narrowly interpreted. Construed broadly, this decision could be persuasive authority for permitting the search of any traveler's computer simply because the traveler passes through customs. The court's statement that all "closed containers" are subject to "routine" searches and do not require reasonable suspicion is problematic because it fails to consider the nature of computer files.[33] This rule would permit a customs agent to search a traveler's computer and diskettes without reasonable suspicion merely because they are considered "closed containers" for the purposes of a Fourth Amendment[34] search.[35] This case comment contends that to search a computer or computer diskette, a customs official must first have reasonable suspicion that the computer or computer diskette contains contraband.

In *Irving*, the court compared the search of a computer diskette to the search of luggage.[36] According to the court, both are considered "closed containers" and therefore come within the scope of a "routine" border search.[37] This analysis is problematic for two reasons. First, simply because luggage, computers, and dis-

33. *See* United States v. Molina-Tarazon, 279 F.3d. 709, 713 (9th Cir. 2000) ("[S]ome searches of inanimate objects can be so intrusive as to be considered nonroutine.").

34. The Fourth Amendment provides:

> The 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, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

35. *See Irving*, 2003 WL 22127913, at *5, *citing* United States v. Roberts, 86 F. Supp. 2d 678, 688-89 (S.D. Texas 2000). In *Roberts*, the defendant was charged with possession of child pornography based on evidence obtained during a warrantless border search. Customs agents received a tip that Roberts would be traveling from Houston to Paris and that he would be in possession of child pornography. When Roberts arrived at the airport, customs inspectors searched him. The inspectors found six Zip computer disks inside Roberts' shaving kit, exactly where the informant said they would be located. Agents then opened Robert's laptop and told him that they needed to scan the material on the disks. The court found that a search of Roberts's computer would not have been "destructive or so personally invasive as to be non-routine." The court came to this conclusion by "analogizing the Fourth Amendment protection afforded to an individual's computer files and computer hard drive to the protection given an individual's closed containers and closed personal effects."

36. *See Irving*, 2003 WL 22127913, at *5.

37. *See id.*

kettes are considered "closed containers" does not automatically mean that they should be subject to a "routine" border search.[38] A single disk may contain large amounts of information relating to many different topics.[39] A more appropriate analogy would compare a computer disk or hard drive to an entire archive or record center.[40] Furthermore, this analogy "oversimplif[ies] a complex area of Fourth Amendment doctrines and ignore[s] the realities of massive modern computer storage."[41] Second, the court's reasoning is problematic because the border-search doctrine turns on whether the search is "routine" or "non-routine," not whether the object is a "closed container."[42]

The border-search doctrine permits government agents to conduct a search at an international border without a warrant, probable cause, or any suspicion to justify the search, as long as the search is "routine."[43] A "routine search" is a search that does not "seriously invade a traveler's privacy."[44] If a traveler's privacy is seriously invaded then the search is considered "non-routine" and reasonable suspicion is required to perform the search.[45] In *United States v. Kelly*,[46] the Fifth Circuit held "the key variable [for determining when a search is 'routine'] is the invasion of the privacy and dignity of the individual."[47]

38. *See Molina-Tarazon*, 279 F.3d. at 713 ("[S]ome searches of inanimate objects can be so intrusive as to be considered nonroutine.").

39. Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 86 (1994) ("Given the massive storage capacities of disks and other modern storage media, a single disk may well contain information on a vast array of topics. For example, officers searching a computer for a telephone number may use the opportunity to rummage through financial records, written correspondence, electronic mail, or other obviously personal and irrelevant records also contained on the computer.").

40. *Id.* at 82.

41. *See* United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999) ("'Relying on analogies to closed containers or file cabinets may lead courts to 'oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage.'") (citation omitted).

42. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985).

43. *Rivas*, 157 F.3d at 367.

44. *Id.*, *citing* United States v. Cardenas, 9 F.3d 1139, 1147 (5th Cir. 1993).

45. *See* United States v. Robles, 45 F.3d 1, 5 (1st Cir. 1995); *see also Rivas*, 157 F.3d at 367.

46. 302 F.3d. 291 (5th Cir. 2002).

47. *Id.* at 294.

Similarly in *United States v. Braks*,[48] the First Circuit held that the degree of invasiveness or intrusiveness involved in the search determines whether the search is "routine."[49] Thus, the main focus of a "routine" search is the degree of intrusiveness involved, and not whether the object searched is a "closed container."[50] Based on the reasoning employed in *Kelly* and *Braks*, the *Irving* court's analysis that the customs agents could have searched Irving's computer diskettes without reasonable suspicion is troubling.[51]

The *Irving* court relied upon *United States v. Roberts*[52] for the proposition that the "inspection of the contents of closed containers comes within the scope of a routine border search and is permissible even in the absence of reasonable suspicion or probable cause."[53] However, there are circumstances in which the search of closed containers could be so intrusive as to be considered nonroutine.[54]

In *United States v. Molina-Tarazon*,[55] the Ninth Circuit held that customs agents' removal, disassembly, and search of the fuel tank on the defendant's pickup truck was not a "routine" border search and therefore required reasonable suspicion under the Fourth Amendment.[56] The Ninth Circuit further stated that it might be difficult to determine when an inanimate object search becomes so intrusive as to warrant reasonable suspicion.[57] A search of an inanimate object does not subject a person to the same degree of indignity as a search of the human body.[58] However, it is important to note that causing indignity is not the only way a search might be

48. 842 F.2d. 509 (1st Cir. 1988).

49. *Id.* at 511.

50. *See id.; see also Kelly*, 302 F.3d. at 294.

51. *Compare Kelly*, 302 F.3d. at 294 (explaining that the requirement of reasonable suspicion in a border search depends on the degree of intrusion into the privacy and dignity of the individual), and *Braks*, 842 F.2d. at 512 (stating that one of the factors for determining the degree of intrusiveness involved in a search is "whether the suspect's reasonable expectations of privacy, if any, are abrogated by the search").

52. 86 F. Supp. 2d 678 (S.D. Texas 2000).

53. *Irving*, 2003 WL 22127913, at *5, *citing Roberts*, 86 F. Supp. 2d at 688.

54. *Molina-Tarazon*, 279 F.3d. at 713 ("[S]ome searches of inanimate objects can be so intrusive as to be considered nonroutine.").

55. 279 F.3d. 709 (9th Cir. 2000).

56. *Id.* at 717.

57. *Id.* at 713.

58. *Id.*

"non-routine." A search could be considered "non-routine" based on the use of force, the risk of harm, and the diminished sense of security that is involved in, or comes about as a result of, the search.[59]

In *Molina-Tarazon*, the court considered whether the search of the defendant's fuel tank was psychologically intrusive when determining if the search was "non-routine."[60] The court stated that "[p]eople's minds are as vulnerable to intrusion as their physical possessions."[61] As a result, fear is a significant factor that needs to be addressed when evaluating the level of intrusiveness involved in a search.[62] The *Molina-Tarazon* court emphasized that "government intrusions into the mind, specifically those that would cause fear or apprehension in a reasonable person, are no less deserving of Fourth Amendment scrutiny than intrusions that are physical in nature."[63] The search of a traveler's computer may cause fear or apprehension because of the potentially large amount of personal information that might be stored in it.[64] Therefore, searching computer files could be psychologically intrusive and contribute to a traveler's apprehension.

The *Molina-Tarazon* court specifically focused on how the search of a fuel tank could contribute to a driver's apprehension.[65] The court's analysis is useful for determining whether the search of

59. *Id.* (explaining that force, harm, and psychological effect of a search happen to be factors relevant in this case, but not ruling out the fact that other factors may also render a search non-routine).

60. *Id.* at 715.

61. *Molina-Tarazon*, 279 F.3d at 715.

62. *Id.* at 716 ("The imposition of fear is a type of psychological intrusion. The Supreme Court has therefore recognized that the level of fear a particular search is likely to engender is a significant factor in evaluating intrusiveness.").

63. *Id.*, *citing* United States v. Martinez-Fuerte, 428 U.S. 543, 588 (holding that fixed checkpoints are preferable to roving searches because "the subjective intrusion — generating of concern or fright on the part of the lawful traveler — is appreciably less. . .."); *cf.* Craig M. Bradley, *Constitutional Protection for Private Papers*, 16 HARV. C.R.-C.L. L. REV. 461, 483 (1981) ("A search for private papers may be no more physically intrusive than a search for a gun, but the psychological intrusion is far greater because the searcher is invading not only the subject's house but his or her thoughts as well.").

64. *See* United States v. Walser, 275 F.3d. 981, 986 (10th Cir. 2001) ("Because computers can hold so much information touching on many different areas of a person's life, there is a greater potential for the 'intermingling' of documents and a consequent invasion of privacy when police execute a search for evidence on a computer.").

65. *Molina-Tarazon*, 279 F.3d. at 716.

a computer should require reasonable suspicion. The court recognized that a driver might not know if the government contractor is licensed to perform the work involved — i.e, removing the fuel tank to search for drugs and then reattaching it — or what standards the government used in selecting a contractor.[66] Similarly, in *Irving*, a traveler may be unaware of the customs agent's computer skill level, and/or the standards used in hiring him to perform the search, thus contributing to a traveler's apprehension. Furthermore, one of the biggest threats to a computer is not a virus or a worm, but rather an accident caused by an unskilled user.[67]

In addition, the *Molina-Tarazon* court noted that there is no independent incentive for a government contractor to act with caution, skill, and precision.[68] Instead, the main concern is to search quickly and find contraband, and not necessarily to act with the greatest of care.[69] This is also analogous to *Irving* because customs agents lack the incentive to take adequate precautions when working on a traveler's computer files. Their purpose is to find illicit materials and not necessarily to act with the greatest of care when dealing with a traveler's computer diskette.

Finally, the *Molina-Tarazon* court addressed the complexity of a search such as the one on Molina's truck and stated that a driver has no way of knowing whether the parts are restored to their original state.[70] Moreover, if no certified or licensed mechanic is present, the driver has no way of confirming whether the fuel tank is correctly reassembled.[71] Similarly, in *Irving*, if no certified or licensed computer technician is present during the search of a traveler's computer, then the traveler has no way of verifying that the

66. *Id.*

67. *See* George V. Hulme, *The Threat From Inside: The Biggest Danger to Computer Systems Comes from Employees. New Products Address the Problem.* (April 14, 2003), *available at* InformationWeek, http://www.informationweek.com/story/showArticle.jhtml?articleID=8900062 (last visited Sept. 9, 2004) ("'Too much attention has been focused on the outside threat,' says Shannon Clyde, an information security officer for Travis County, Texas. 'I'm just as worried about 'Joan' in accounting making a naïve mistake and trashing financial spreadsheets or making information available where it shouldn't be.'").

68. *Molina-Tarazon*, 279 F.3d. at 716 (explaining why a driver might have reason to doubt a mechanic's incentive to take adequate precautions in dismantling and reassembling portions of the vehicle).

69. *Id.*

70. *Id.* at 717.

71. *Id.*

computer was returned to its original state, and that no files are missing or damaged. Therefore, the increased level of psychological intrusiveness and apprehension involved in searching a traveler's computer files supports the need for a reasonable suspicion requirement.

In addition to the psychological intrusion and apprehension involved in searching a computer, the intrusion involved in a close reading of computer files, absent reasonable suspicion, could also violate a person's privacy rights.[72]

In *United States v. Soto-Teran*,[73] the court recommended the application of a reasonable suspicion standard for determining the lawfulness of a border officials' actions when closely reading and photocopying documents.[74] The court stated that the perusal of mail, letters, and documents falls within a routine border search, yet a closer, more careful examination of those documents could intrude on a person's privacy because they may contain sensitive personal information, such as a diary or desk calendar.[75] Similarly, in *Irving*, a close reading of computer files intrudes on a person's privacy because those files could deal with the same personal matters. Computers often contain confidential information.[76] Additionally, computers are now frequently used for business purposes and often contain confidential corporate information.[77] Furthermore, because privacy expectations "[relate] to the contents of [a] container rather than to the container itself,"[78] placing data in a computer or on a diskette creates a reasonable expectation of privacy in the contents of that container.[79] Additionally, because a

72. *See* United States v. Soto-Teran, 44 F. Supp. 2d. 185, 191 (E.D.N.Y. 1996).

73. 44 F. Supp. 2d. 185 (E.D.N.Y. 1996).

74. *Id.* at 191.

75. *Id.*

76. *See* Winick, *supra* note 39, at 81 ("[C]omputers are repositories of personal information.").

77. *See* Baer v. Reliant Energy Mid-Atlantic Power Holdings, 2002 WL 31189503, at *5 (E.D. Pa. 2002) ("Many people in today's workforce use computers for their jobs. . ."); *see also, e.g.,* Prowest Diversified, Inc. v. United States, 40 Fed.Cl. 879, 885. (1998) ("[Attorney] entered the billing information directly onto a computer program, which generates billing statements to clients.").

78. United States v. Barth, 26 F. Supp. 2d 929, 936 (W.D. Tex 1998).

79. *Id.* at 936-37 ("By placing data in files in a storage device such as his hard drive, the [c]ourt finds that Defendant manifested a reasonable expectation of privacy in the contents of those files.").

computer can hold a large amount of personal information, there is great potential for the invasion of privacy when the government executes a search for evidence on a computer.[80] Therefore, a reasonable suspicion standard should be applied to computer searches in the border context because of the increased potential for the invasion of privacy.

The *Irving* court managed to avoid the issues raised in this case comment by finding reasonable suspicion.[81] Although a search that is not "routine" requires a reasonable suspicion of wrongdoing,[82] determining whether a search is "routine" or "non-routine" is irrelevant if reasonable suspicion is already present.[83] A reasonable suspicion of wrongdoing was present in *Irving* because Irving was already the subject of a government investigation and was in possession of children's books and drawings at the time the customs inspector initially searched his bags.[84] Thus, in *Irving,* it did not matter whether the search was "routine" or "non-routine" because the reasonable suspicion of wrongdoing was already present.[85]

Irving should be narrowly construed to apply only to cases where reasonable suspicion is present because of the fear and apprehension a traveler may face when a customs agent searches a computer.[86] Furthermore, the reasonable suspicion standard normally applied to "non-routine" searches should be used in all border searches of computers because of the increased potential for an invasion of privacy.[87] Requiring the reasonable suspicion standard will thus prevent *Irving*'s dicta from providing the basis for a troubling expansion of the border-search doctrine.

80. *Walser*, 275 F.3d. at 986 ("Because computers can hold so much information touching on many different areas of a person's life, there is a greater potential for the 'intermingling' of documents and a consequent invasion of privacy when police execute a search for evidence on a computer.").

81. *See Irving*, 2003 WL 22127913, at *5.

82. *See Rivas*, 157 F.3d at 367.

83. *See Molina-Tarazon*, 279 F.3d. at 717 ("That the search was not routine does not necessarily render it unlawful. The search would still have been lawful if the officers conducted it based on a reasonable suspicion that Molina might have been concealing contraband.").

84. *Irving*, 2003 WL 22127913, at *5.

85. *Id.*

86. *See Molina-Tarazon*, 279 F.3d. at 716-17.

87. *See Walser*, 275 F.3d. 986 (arguing that there is a potential invasion of privacy involved in a computer search); *see also Soto-Teran*, 44 F. Supp. 2d. at 191.