New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
Web address: http://www.nylj.com
VOLUME 239—NO. 87 TUESDAY, MAY 6, 2008 ALM

WHITE-COLLAR CRIME

BY ELKAN ABRAMOWITZ AND BARRY A. BOHRER

Expansion of Border Searches to Laptops, Electronic Items

The government has increased its focus on border security in response to heightened concerns of international terrorism and crime. Accordingly, international business travelers may be subject to more extensive searches when leaving and entering the United States.

We have previously written that "the rules applicable to government searches of offices, homes, and motor vehicles are by now reasonably clear. Much less certain, however, are the standards that govern searches and seizures of computers."[1] Recent decisions reflect that the extent to which the government can search items such as laptop computers, BlackBerries, and other devices remains unresolved.

'Elect. Frontier Foundation' Case

In February 2008, the Electronic Frontier Foundation and Asian Law Caucus filed suit against the U.S. Department of Homeland Security for denying access to public records on the questioning and searches of travelers at U.S. borders.[2] According to the plaintiffs, the suit was filed in response to growing complaints of "excessive or repeated screenings by U.S. Customs and Border Protection agents." Complaints filed with these public service organizations assert that the agents not only

Elkan Abramowitz *Barry A. Bohrer*

questioned individuals extensively, but also examined their "books, business cards collected from friends and colleagues, handwritten notes, personal photos, laptop computer files, and cell phone directories," sometimes making copies of this information.[3]

The government "maintains that it has a virtually unlimited power to examine the contents of any electronic storage device moving into or out of the country."[4] The government purports to derive its power from regulations implemented by the secretary of Treasury that provide for the search and inspection of all "persons, baggage, and merchandise" entering the United States from a foreign country.[5] Indeed, in *United States v. Montoya de Hernandez,* the U.S. Supreme Court recognized that the Fourth Amendment does not prohibit routine, warrantless searches as part of a reasonable border search. No probable cause or reasonable suspicion of criminal activity is required.[6] Airport terminals have been determined to be the "functional equivalent" of borders, and rules applying to passengers flying into the United States also apply to passengers leaving the country on international flights.[7]

The key language in the Supreme Court's opinion in *Montoya de Hernandez* focuses on the Fourth Amendment's nonapplication to routine searches. Lower courts interpreting and applying the case have seized on this language, recognizing two different categories of border searches, routine and nonroutine. Nonroutine searches are those that involve a high degree of intrusion, such as a strip search, and require the government to have some particularized and objective basis for subjective wrongdoing in order to conduct the search. This standard often is referred to as "reasonable suspicion."[8]

It is unclear whether searches of laptop computers are routine or nonroutine. Accordingly, it is unclear whether the government is required to demonstrate a heightened standard of cause when searching laptops and similar devices during border searches. In March 2008, the Congressional Research Service prepared a report for Congress on "Border Searches of Laptops and Other Electronic Storage Devices." The report concluded that "[t]hough the federal courts have universally held that the border search exception applies to laptop searches conducted at the border, the degree of cause required to support the search has not been established."[9]

Written opinions on the issue derive primarily from cases involving individuals who are found to have child pornography on their computer during a border search. Although not the classic white-collar scenario, these cases are instructive on how courts are analyzing the issues related to border searches of portable data storage devices. Given the various outcomes of these cases, they also demonstrate the degree of uncertainty in this area of law.

Fourth Circuit: 'Ickes'

In *United States v. Ickes*,[10] the defendant was convicted of transporting child pornography in the U.S. District Court for the Eastern District of Virginia. The evidence against Mr. Ickes was obtained by border agents during a search of Mr. Ickes' van while he was attempting to enter the United States from Canada. A thorough search of the van revealed a Virginia state arrest warrant for Mr. Ickes, marijuana, and several albums containing photographs of provocatively posed prepubescent boys in

Elkan Abramowitz *is a member of Morvillo, Abramowitz, Grand, Iason, Anello & Bohrer. He is a former chief of the criminal division in the U.S. Attorney's Office for the Southern District of New York.* **Barry A. Bohrer** *is also a member of Morvillo, Abramowitz and was formerly chief appellate attorney and chief of the major crimes unit in the U.S. Attorney's Office for the Southern District of New York.* **Gretchan R. Ohlig,** *an attorney, assisted in the preparation of this article.*

various stages of undress. Mr. Ickes was then placed under arrest and detained. During his detention, the agents continued to search the defendant's van, seizing his computer and 75 computer disks, one of which contained incriminating videos of Mr. Ickes with underage children.

Prior to trial, Mr. Ickes sought the suppression of the evidence collected from his computer and the disks, alleging that the warrantless search violated his First and Fourth amendment rights. The district court denied his motion, holding that the search fell under the extended border search doctrine, an established exception to the Fourth Amendment warrant requirement. Mr. Ickes appealed his subsequent conviction arguing that the district court's decision denying his request for suppression was erroneous.

In examining the defendant's claim, the U.S. Court of Appeals for the Fourth Circuit looked at the "sweeping" language through which Congress empowered customs officials. Specifically, §1581(a) of Title 19 states that "[a]ny officer of the customs may at any time go on board of any vessel or vehicle at any place in the United States …or at any other authorized place…and examine, inspect, and search the vessel or vehicle and every part thereof and any person, trunk, package, or cargo on board…."

Mr. Ickes argued that this language was insufficient to cover the search of his computer and disks because it did not explicitly mention electronic equipment, which he believed to be an intentional omission. The Court of Appeals rejected this argument, finding that the computer and disks were "cargo," defined in Black's Law Dictionary as "goods transported by a vessel, airplane, or vehicle." "To find otherwise would undermine the long-standing practice of seizing goods at the border even when the type of good is not specified in the statute."[11]

The court then addressed the rationale for allowing such expansive border searches. Observing that the government has an overriding interest in securing the safety of its citizens by seeking to prevent the introduction of contraband or criminals into the country, the court noted that individuals approaching the border have a reduced expectation of privacy. "When someone approaches a border, he should not be surprised that '[c]ustoms officers characteristically inspect luggage…; it is an old practice and is intimately associated with excluding illegal articles from the country.'"[12] For these reasons, the court rejected Mr. Ickes' argument that there should be a First Amendment exception to the broad border search authority when the search involves "expressive" material.

Mr. Ickes further argued that the district court's ruling meant that any person carrying a laptop computer on an international flight would be subject to a search of the files on the computer hard drive. The Court of Appeals found this prediction "far-fetched," noting that custom agents do not have the time or resources to search every computer. Rather, the court pointed out that in Mr. Ickes' case, the agents did not search the defendant's computer until after they had discovered drug paraphernalia, photo albums and a video of child pornography, and an outstanding warrant for Mr. Ickes' arrest. "As 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."[13] For all these reasons, the court affirmed the district court's decision and Mr. Ickes' conviction.

Ninth Circuit: 'Arnold'

In *United States v. Arnold*, the U.S. District Court for the Central District of California entertained a defendant's motion to suppress evidence obtained from a search of his laptop, hard drive, CDs, and memory stick at Los Angeles International Airport. The defendant was indicted for transportation of child pornography and possession of a computer hard drive and compact discs containing images of child pornography. Granting the defendant's motion, the district court's opinion was the first and only to find laptop searches to be nonroutine, requiring a showing of reasonable suspicion.[14]

The District Court found that opening and viewing confidential computer files implicated significant dignity and privacy interests and that the Fourth Amendment required the government to possess a reasonable suspicion to perform such an intrusive search. The District Court rejected the government's argument that the search was routine and did not require a showing of reasonable suspicion because the defendant's tangible property, and not his person, was searched. Rather, the District Court held that the search of a computer or similar storage device, and the information contained thereon, was "substantially more intrusive than a search of the contents of… other tangible objects":

> A laptop and its storage devices have the potential to contain vast amounts of information. People 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. In this case, [Mr.] Arnold kept child pornography on his laptop and in his storage devices; however, "[i]t is a fair summary of history to say that the safeguards of liberty have frequently been forged in controversies involving not very nice people."[15]

Recently, the Ninth Circuit reversed this decision, finding that "reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage device at the border."[16] In so finding, the court noted that other than when "intrusive searches of the person" are at issue, the Supreme Court has held open the possibility, "'that some searches of property are so destructive as to require' particularized suspicion."[17]

That being said, the Court said that the district court's use of a "sliding intrusiveness scale" to determine when reasonable suspicion is required was misplaced because it was a scale created in cases involving the search of persons rather than property. "The Supreme Court has stated that '[c]omplex 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.'" In fact, the Ninth Circuit rejected the notion that the "routine" versus "nonroutine" distinction was at all applicable to searches of property.[18]

In examining the Supreme Court's language in *Flores-Montano*, the Ninth Circuit found that there were only two possible circumstances that would require reasonable suspicion for a border search of property: (i) where there is "exceptional damage to property" or (ii) where the search is conducted in a "particularly offensive manner." Noting that Mr. Arnold did not claim either of these circumstances, the court concluded that no reasonable suspicion was required for the search of his laptop. Finally, the court rejected the defendant's arguments that the search of his laptop could be analogized to a home search. Accordingly, the decision granting Mr. Arnold's motion

to suppress the evidence resulting from the search of his laptop was reversed.[19]

Additional Concerns

The Fourth Circuit implied in *Ickes* that laptop searches fell within the routine border exception to the Fourth Amendment requirements, but reasoned that the specific search at issue in that case was nonetheless supported by reasonable suspicion. The Ninth Circuit's decision in *Arnold* expands circuit law in finding that the electronic contents of an international traveler's laptop may be searched without any reasonable suspicion, rejecting the application of the routine versus nonroutine search distinction. However, other circuits, including the Second Circuit, continue to examine the issue based on whether the search can be classified as "routine" or "nonroutine." In *United States v. Irving*, the Second Circuit said that "the level of intrusion into a person's privacy is what determines whether a border search is routine" and that "[a] border search is valid under the Fourth Amendment, even if nonroutine, if it is supported by reasonable suspicion."[20] Clearly, the answer to the question whether the border search of a laptop computer implicates the Fourth Amendment is less than pellucid.

In addition, intrusive border searches also may implicate the Fifth Amendment and issues related to statutory and common-law privileges.[21] A recent case in Vermont demonstrates how Fifth Amendment concerns might come into play. In December 2006, customs agents working at the Canadian/U.S. border in Vermont seized a computer belonging to Sebastien Boucher and arrested him on a complaint charging him with transportation of child pornography. Soon thereafter, the government determined that the relevant computer files were encrypted, password-protected, and inaccessible. As a result, the grand jury subpoenaed Mr. Boucher to enter a password to allow access to the files on the computer. Mr. Boucher moved to quash the subpoena on the grounds that it violated his Fifth Amendment privilege.

After a two-day evidentiary hearing, a magistrate judge granted Mr. Boucher's motion to quash the subpoena, ruling that compelling Mr. Boucher to enter his password would violate his Fifth Amendment privilege against self-incrimination. "If [Mr.] Boucher does know the password, he would be faced with the forbidden trilemma: incriminate himself, lie under oath, or find himself in contempt of court."[22] The government has appealed this decision to the District Court of Vermont and commentators have expressed doubt about the validity of the magistrate judge's ruling, including some who believe Mr. Boucher lost his Fifth Amendment privilege when he admitted the computer was his and that he stored images in the encrypted part of the hard drive.[23]

Finally, observers note that attorneys who carry privileged information during international travel have cause for concern that this information may be divulged in contravention of their ethical duty to maintain client confidences. The same is true of many business travelers who have confidential, proprietary information in their possession. To avoid these issues, some suggest minimizing the amount of such information kept in portable devices or accessing the information remotely through the Internet or other network systems.[24]

Conclusion

International travelers and portable electronic devices they carry are being exposed to more scrutiny by law enforcement agents. Until issues addressing the legitimacy of these border searches are resolved, travelers should handle privileged and proprietary information as if it will be subject to unlimited searches at international borders. The authors' previous observation holds true: "the application of traditional Fourth Amendment rules to the seizure and use of digitized evidence can potentially result in less than satisfactory conclusions of law."[25]

1. Elkan Abramowitz and Barry A. Bohrer, "The Fourth Amendment in the Age of the Computers," NYLJ, Nov. 7, 2006, Volume 236-No. 89.
2. *Asian Law Caucus and Electronic Frontier Foundation v. U.S. Dept. of Homeland Security,* CV 08-0842 (N.D. California).
3. Electronic Frontier Foundation Web site, http://www.eff.org/cases/foia-litigation-border-searches.
4. Ronald Lee, Robert Litt and Stephen Marsh, "Do Privacy Rights Extend to International Travelers? Warrantless Border Searches of Electronic Devices," BNA Privacy and Security Law Report, Vol. 07, No. 08 (Feb. 25, 2008).
5. 19 U.S.C. §1582; 19 C.F.R. §162.6.
6. *United States v. Montoya de Hernandez,* 473 U.S. 531, 38 (1985).
7. *United States v. Okafor,* 285 F.3d 842, 45 (9th Cir. 2002); *United States v. Romm,* 433 F.3d 990, 96 (9th Cir. 2006).
8. Yule Kim, "Border Searches of Laptops and Other Electronic Storage Devices," CRS Report for Congress (March 5, 2008).
9. Kim, "Border Searches of Laptops and Other Electronic Storage Devices."
10. 393 F.3d 501 (4th Cir. 2005).
11. Id. at 505.
12. Id. at 506 (citing *United States v. Thirty-Seven Photographs,* 402 U.S. 363, 76 (1971)).
13. Id. at 507.
14. *United States v. Arnold,* 454 F.Supp.2d 999, 1000 (C.D.Ca. 2006).
15. Id. at 1004 (citations omitted).
16. __F.3d__, 2008 WL 1776525 (9th Cir. April 21, 2008).
17. Id. at *3 (citing *Flores-Montano,* 541 U.S. at 152).
18. Id.
19. Id. at **5-6.
20. 452 F.3d 110, 123-124 (2nd Cir. 2006).
21. Lee, et al., "Do Privacy Rights Extend to International Travelers?"
22. *In re Boucher,* 2007 WL 4246473, *3 (D.Vt. Nov. 29, 2007).
23. Ellen Nakashima, "In Child Porn Case, a Digital Dilemma," Washington Post (Jan. 16, 2008).
24. Kim, "Border Searches of Laptops and Other Electronic Storage Devices;" Joe Sharkey, "At U.S. Borders, Laptops Have No Right to Privacy," New York Times (Oct. 24, 2006).
25. Elkan Abramowitz and Barry A. Bohrer, "The Fourth Amendment in the Age of the Computers," NYLJ, Nov. 7, 2006, Volume 236-No. 89.