BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Warrantless Searches

International Travel

Do Privacy Rights Extend to International Travelers? Warrantless Border Searches of Electronic Devices

BY RONALD LEE, ROBERT LITT, AND STEPHEN MARSH

International travelers may be surprised to learn that the U.S. government claims the authority to review the contents of laptop computers, Blackberries®, PDAs, cellphones, and other electronic storage devices when a person enters this country. For international business travelers, this is an especially disquieting development, as it could potentially result in the unanticipated disclosure of sensitive, and in some cases, legally privileged, confidential information.

The assertion of this far-reaching authority by the government raises a number of legal issues. The most obvious one is the government's power under the Fourth Amendment to conduct a border search of a laptop computer or other electronic storage device without a warrant or even a reasonable suspicion of criminal activity. But because the government also claims the right to compel an individual to reveal a computer password as part of a border search, the scope of an individual's Fifth Amendment right against compelled self-incrimination has also been drawn into question. On top of these constitutional concerns are serious questions about the impact these searches may have on claims of statutory or common law privilege, such as the attorney-client privilege or attorney work product doctrine.

These are not mere theoretical issues. The U.S. government's efforts to prevent international terrorists and criminals from entering the country have intensified since the Sept. 11, 2001 terrorist attacks and are likely to continue. This increased focus on border security has taken place during a period in which there was near exponential growth in portable information technology. As society increasingly craves more and more information, computers and other similar devices have become the central hub for our interactions with the world at large. We use them to draft documents, create presentations, communicate with colleagues, and organize vast quantities of critical information. Computers, Blackberries®, and cellphones often contain vast amounts of personal, historical and possibly confidential data, yet because they play such a central role in conducting our day-to-day affairs, they cannot easily be left behind when we travel. The need to use our electronic storage devices wherever we go has also spurred technological advances in accessing data from remote locations. Whether a traveler connects directly to her corporate network at a foreign office or uses high-speed

 ISSN 1538-3423

wireless Internet connections, she can essentially carry her virtual world with her wherever she goes.[1]

That virtual world can include a great deal of information that is sensitive in nature, including proprietary data, medical and financial records, and privileged communications, to name but a few examples. Carrying that information across the border is unavoidably problematic because the U.S. 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. Travelers, however, are beginning to take notice. Recent news reports have highlighted border searches involving electronic storage devices and concerns that these searches may be prompted in part by the race, ethnicity, or national origin of the traveler. Some travelers have also complained that government officials have deleted or altered data during border searches of these electronic items.[2] Two public interest groups recently filed suit in federal court to determine the scope of the government's authority to search laptops and other electronic devices during border searches.[3]

To understand the complexities of the arguments for and against the government's position on limitless border searches, we explore the following issues: whether the government has the constitutional authority to conduct warrantless searches of the contents of an electronic storage device during a border search; whether the government has the power to compel an individual to supply his or her password or passwords so that the government can search the encrypted hard drive or individually encrypted files of the device in question; whether a traveler carrying potentially privileged material puts such a privilege at risk by carrying that material during international travel; and what options travelers have, with what potential consequences, when the government seeks to search an electronic storage device at the border.

1. *The Government's Border Search Authority*

Federal law expressly authorizes customs officials to detain and search individuals coming into the United States from foreign countries.[4] And the Fourth Amendment does not prohibit customs agents from engaging in routine, warrantless searches of individuals and their belongings as part of a reasonable border search, even where there is no probable cause or reasonable suspicion of criminal activity.[5] Border searches are deemed to be reasonable ''simply by virtue of the fact that they occur at the border,''[6] where the government has a compelling interest in regulating the collection of duties and protecting itself from ''the entry of unwanted persons and effects . . . .''[7] Because international airport terminals are considered the ''functional equivalent'' of borders,[8] ''passengers deplaning from an international flight are subject to routine border searches.''[9] The same rules apply to passengers leaving the country on international flights.[10]

Placing a computer in a x-ray scanner and examining it to see if it contains some sort of explosive device clearly falls within the government's border authority. But allowing the government to turn a computer on and examine its contents is a far more intrusive search. Courts have struggled to determine the extent of the government's border search authority, with much of the confusion originating with the Supreme Court's opinion in *United States v. Montoya de Hernandez*. That decision implicitly suggested that individualized suspicion of wrongdoing would only be needed to justify ''nonroutine'' border searches.[11] Lower courts developed complex balancing tests to determine whether particular types of border searches qualified as ''nonroutine,'' thereby requiring a higher level of individualized suspicion.[12] When courts began to apply these tests to

[1] Airlines, eager to lure high-margin international business travelers, are adding high-speed wireless Internet connectivity on some transcontinental flights, thereby making it easier for business travelers to work en route to their ultimate destination. Katherine Noyes, *AA to Lure Business Travelers with Whiff of Wi-Fi*, TECHNEWSWORLD, Aug. 2, 2007, available at http://www.technewsworld.com/story/58644.html (discussing American Airlines plan to add limited Internet connectivity for international business travelers). Singapore Airlines has even added a service that allows travelers to plug in ''flash drives'' to an existing system so that the users can work on the plane without even opening their own computers. Aaron Tan, *Star Office Flies with S'Pore Airlines*, ZDNETASIA, June 1, 2007, available at http://www.zdnetasia.com/news/software/0,39044164,62017780,00.htm.

[2] *E.g.*, Ellen Nakashima, *Clarity Sought on Electronics Searches*, WASHINGTON POST, Feb. 7, 2008, at A01.

[3] Jeanne Meserve, *Suit: Airport Searches of Laptops, Other Devices Intrusive*, CNN, Feb. 11, 2008, http://www.cnn.com/2008/TRAVEL/02/11/laptop.searches/index.html (discussing federal lawsuit filed by Electronic Frontier Foundation and Asian Law Caucus to clarify government's authority to review contents of electronic storage devices during border searches).

[4] *See* 19 U.S.C. § 1582 (conferring authority on Secretary of Treasury to implement regulations governing border searches); 19 C.F.R. § 162.6 (providing that all ''persons, baggage, and merchandise'' entering the United States from a foreign country is subject to search and inspection by customs officials).

[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. Flores-Montano*, 541 U.S. 149, 152 (2004); *see also Montoya de Hernandez*, 473 U.S. at 537.

[8] *United States v. Okafor*, 285 F.3d 842, 845 (9th Cir. 2002).

[9] *United States v. Romm*, 455 F.3d 990, 996 (9th Cir. 2006).

[10] *Cf. United States v. Ezeiruaku*, 936 F.2d 136, 143 (3d Cir. 1991) (applying traditional rationale for border searches to outgoing border search context); *United States v. Duncan*, 693 F.2d 971, 977 (9th Cir. 1982) (''Since this was a search at a 'border', of a person leaving the country, there is no need for probable cause, warrants, or even suspicion.''); *United States v. Ajlouny*, 629 F.2d 830, 834 (2d Cir. 1980) (applying border search exception to items leaving the country as well as those entering the country).

[11] *Montoya de Hernandez*, 473 U.S. at 538, 541 n.4 (noting that ''routine'' border searches were permissible without a warrant or any reasonable suspicion but refusing to opine on the question of what level of suspicion would justify ''nonroutine'' border searches, such as a strip or body cavity search).

[12] *Compare United States v. Vance*, 62 F.3d 1152, 1156 (9th Cir. 1995) (concluding that ''pat down'' search, which required individual to be spread out against a wall, had to be justified by ''minimal suspicion'' of criminal conduct) *with Bradley v. United States*, 299 F.3d 197, 203-04 (3d Cir. 2002) (concluding that ''standard'' patdown search was a ''routine'' search that did not require individualized suspicion).

  PVLR ISSN 1538-3423

searches of physical containers rather than persons,[13] the Supreme Court stepped back into the fray.

In *United States v. Flores-Montano*, the Court had to decide whether customs inspectors at the U.S.-Mexico border had the authority, without any probable cause or reasonable suspicion, to disassemble the gas tank of a traveler's vehicle in order to see if it contained illegal contraband. The Court expressly rejected the Ninth Circuit's approach, which focused on whether the search was ''routine'' in light of the ''degree of intrusiveness'' involved.[14] ''[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.''[15]

Seizing on this language from *Flores-Montano*, the government contends that it has virtually unlimited authority to search any type of physical container, whether that container is a fuel tank or a computer, insisting that this authority is necessary to protect the country from potential terrorist attacks and other threats to public safety.[16] That position has been endorsed by the Fourth Circuit, which specifically noted that the government's border search authority, including the authority to search computers, ''is justified by'' the government's ''national security interests,'' interests that ''may require uncovering terrorist communications . . . .''[17]

But is it reasonable to view a computer as just another type of ''container,'' analogizing the contents to what one might try to conceal in a suitcase or fuel tank? Critical distinctions can be drawn between computers and other types of storage containers. First, and perhaps most importantly, a computer or other electronic storage device contains far more information than any physical storage container, with a typical computer storing as much information as many libraries.[18] Because computers are repositories for so much information, there is a greater likelihood that they will contain private, confidential information, making them qualitatively different than a fuel tank or other physical container. Second, when a person travels with documents or other types of physical items in a discrete container, there is a greater chance that the traveler has made a conscious decision to carry those items. With a computer, on the other hand, the sheer amount of information means that much of it is simply along for the ride. In fact, as one commentator noted, ''[c]omputers are remarkable for storing a tremendous amount of information that most users do not know about and cannot control,''[19] so that in many cases, a person traveling with a computer could be carrying private, confidential information without any conscious awareness of that fact.

In a case presently pending before the Ninth Circuit, *United States v. Arnold*, a federal district court concluded that computers are substantively different than other containers and that the government cannot examine the contents of such a device in the absence of a warrant or some sort of reasonable suspicion of criminal activity. The district court, in granting a motion to suppress child pornography seized during a border search, observed that laptop computers contain ''all types of personal information,'' including diaries, correspondence, medical information, financial records, attorney-client communications, and trade secrets, among other things. Because of the quantity and type of information contained in many computers, the court held that the search of a computer is inherently ''more intrusive than a search of the contents of a lunchbox or other tangible object,'' thus requiring some degree of reasonable suspicion to justify the search.[20]

Whether *Arnold* survives appellate review depends on whether courts continue to accept the government's argument that intrusive searches are permissible so long as they involve physical objects, not persons. That is not the only possible, or indeed reasonable, interpretation of the Supreme Court's border search jurisprudence. Indeed, the Court's decision in *Flores-Montano* could be read as reflecting the common sense notion that an ''intrusive'' search of a fuel tank is not an ''intrusion'' into one's zone of privacy. A warrantless search of a computer, on the other hand, has far more potential to invade an individual's personal privacy, in certain ways more than a physical search of his person. If, as the Court has suggested, the focus should be on ''the dignity and privacy interests of the person being searched,''[21] courts could logically require the government to establish some level of suspicion before examining the contents of a traveler's electronic storage device during a border crossing.

There is also the possibility that courts, balancing the competing interests, could attempt to strike a middle ground, permitting the government to engage in *limited* perusals of electronic files. The Ninth Circuit, for instance, upheld the government's authority to search international FedEx packages using a ''scanning protocol'' that did not involve detailed examination of any of the documents contained in the packages.[22] A court could conclude that a similar protocol employed to review computers and other electronic storage devices could strike the appropriate balance between protecting the government's legitimate public safety interests and

---

[13] *See, e.g. United States v. Molina-Tarazon*, 279 F.3d 709 (9th Cir. 2002) (concluding that Fourth Amendment precluded government from searching traveler's fuel tank absent reasonable suspicion); *United States v. Rivas*, 157 F.3d 364 (5th Cir. 1998) (holding that reasonable suspicion is necessary for the government to drill into a trailer).

[14] *Flores-Montano, supra* note 7, at 152 (quoting *Molina-Tarazon*, 279 F.3d at 712-13).

[15] *Id.*

[16] *Cf.* Brief for the Gov't-Appellant at 37, 47, *United States v. Arnold*, No. 06-50508, 2007 WL 1407234, at *37, 47 (9th Cir. Mar. 29, 2007) (arguing that computers are ''conceptually identical to closed storage containers'' and noting the government's paramount interest in ensuring our national security).

[17] *United States v. Ickes*, 393 F.3d 501, 506 (4th Cir. 2005); *accord United States v. Linarez-Delgado*, No. 06-2876, 2007 WL 4525200, at *1 (3d Cir. Dec. 19, 2007) (concluding that government's review of contents of camcorder was a permissible exercise of agents' authority to conduct routine border search).

[18] Orin Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 542 (2005).

[19] *Id.* (discussing the fact that computers often contain what are misleadingly known as ''deleted'' files, files which have ostensibly been thrown away but which remain in the digital memory of the computer until they are overwritten).

[20] *United States v. Arnold*, 454 F. Supp.2d 999, 1003-04 (C.D. Cal. 2006), *appeal docketed*, No. 06-50581 (9th Cir. Sept. 17, 2006).

[21] *Flores-Montano*, 541 U.S. at 152.

[22] *United States v. Seljan*, 497 F.3d 1035, 1043-44 (9th Cir. 2007).

preserving some measure of individual privacy. Of course, it is not clear that such a protocol would be workable, because the asserted government interests in examining a computer—to inform the decision whether to admit the passenger into the United States, to protect the public from dangerous materials, and to discover instrumentalities of crime—might not be satisfied without examination of the content of at least some computer files as well as of a directory of programs and file names. Until consistent judicial standards are adopted, the government will likely continue pushing for unlimited authority to search computers and other similar devices when travelers leave or re-enter the country.

2. *Compelled Production of a Computer Password*

Even where the government claims the authority to search a traveler's computer as part of a border search, it may lack the ability to conduct the search because the contents of the device have been encrypted so that they can be accessed only by a password known to the person in possession of the device. In at least one recent case, the government has argued that in addition to its authority to search a computer, it has the power to compel an individual to supply the password so that documents on the computer can be examined.

In that case, *In re Boucher*,[23] the defendant was charged with transporting child pornography after agents conducted a border search of his computer when he attempted to enter the United States from Canada. The initial examination of the computer revealed file names that indicated the likely presence of child pornography on the computer. However, the government was unable to open the files to examine the contents because they had been encrypted.

The government asked the court to order the defendant to produce the password. At first, the government sought to force Boucher to provide the password to the grand jury. Recognizing that this conduct could be deemed testimonial, in violation of Boucher's Fifth Amendment right to avoid compelled self-incrimination, the government later modified its request and asked the court to compel Boucher to type the password into the computer so that its contents could then be examined.

A federal magistrate judge rejected the government's request, concluding that even the compelled entry of the password would violate the defendant's Fifth Amendment rights. One of the key issues was whether the defendant, by typing in the password, would be engaging in a ''testimonial'' communication. The court concluded that such an act would be testimonial, likening it to providing a combination to a locked safe.[24] In the court's view, inputting the password would communicate information about the defendant's knowledge of the password and his access to the subject files, information that could be used to incriminate him. The court, therefore, held that the defendant did not have to supply the password in response to the government's demand.[25]

The government has filed an objection to the magistrate judge's recommendation in *Boucher*,[26] and some commentators have already expressed doubt about the validity of the court's ruling. They note that the court failed to acknowledge that in light of the defendant's prior admissions about ownership and control of the computer, his control of the computer and its contents was a ''foregone conclusion.''[27] Therefore, they argue that any ''testimonial'' aspect supplying the password might otherwise have is irrelevant to the resolution of this case.[28]

Even if *Boucher* is ultimately reversed, this Fifth Amendment issue is likely to arise again. In some cases, for instance, it may not be clear that the government has ''compelled'' the production of the password. Merely asking for it as part of a request to search a computer is unlikely to qualify as the sort of ''custodial'' interrogation that would support a claim of compulsion under the Fifth Amendment.[29] Genuine questions will also arise about whether supplying a password would be incriminating in slightly different factual settings. Even where the production of evidence has some sort of communicative aspect, and hence is ''testimonial,'' it can be difficult to determine whether the testimonial aspect of the production is ''incriminating.'' The Supreme Court has rejected any sort of categorical approach to that question, instead relying on an assessment of the facts of each case.[30] In *Boucher,* the defendant made admissions about his ownership and control over specific files believed to contain child pornography; what happens when the government seizes a computer from a person who fails to provide such admissions? In that latter situation, the compelled production of a password may more clearly be viewed as a ''testimonial'' and incriminating communication because it could be used to prove the defendant's control and access to files in a situation where control and access are not otherwise independently established.

3. *Protection of Privileged Information*

One of the most disconcerting aspects of the government's assertion of authority to search electronic devices at the border is the potential effect such a policy could have on privileged materials, including communications protected by the attorney-client privilege. These concerns affect both lawyers and clients who engage in

[23] *In re Boucher*, No. 2:06-mj-91, 2007 WL 4246473 (D. Vt. Nov. 29, 2007).

[24] *Id.* at *4 (citing *Doe v. United States*, 487 U.S. 201, 210 n.9 (1988) and *United States v. Hubbell*, 530 U.S. 27, 43, (2000)).

[25] *Id.*

[26] Gov't Appeal of Magistrate Judge's Recommendation Granting Def.'s Motion to Quash Subpoena, Case No. No. 2:06-mj-91 (D. Vt. Jan. 2, 2008).

[27] *See, e.g.*, Posting of Orin Kerr to Volokh Conspiracy, http://volokh.com/archives/archive_2007_12_16-2007_12_22.shtml#1197763604 (Dec. 19, 2007, 4:38 EST) (discussing *Boucher* and proper application of ''foregone conclusion'' exception to self-incrimination privilege); Sherry F. Colb, Does the Fifth Amendment Protect the Refusal to Reveal Computer Passwords? In a Dubious Ruling, a Vermont Magistrate Judge Says Yes, FindLaw, Feb. 4, 2008, http://writ.news.findlaw.com/colb/20080204.html

[28] *Cf. United States v. Fisher*, 425 U.S. 391, 410 (1976) (concluding that defendants' production of documents was not ''testimonial'' because the existence and control of the documents was a ''foregone conclusion,'' thereby rendering any communicative aspects of the production irrelevant).

[29] *Cf. United States v. Butler,* 249 F.3d 1094, 1100 (9th Cir. 2001) (holding that detaining a person in a border station's security office from which he or she is not free to leave is not ''custody'').

[30] *United States v. Fisher*, 425 U.S. 391, 410 (1976).

  PVLR ISSN 1538-3423

international travel while in possession of potentially privileged materials. Traveling with privileged materials is an inevitable part of modern life. In some cases, international transportation of privileged material may be necessary to obtain or provide effective legal representation. In other instances, clients and lawyers engaged in international travel may not even be conscious of the fact that their electronic storage devices contain privileged matter.

From the client's perspective, traveling with privileged materials raises the possibility that any privilege will be inadvertently waived in the event that the client consents to government examination of the client's computer. ''[I]f a client wishes to preserve the privilege, it must treat the confidentiality of attorney-client communications like jewels—if not crown jewels.''[31] Where a client gives government officials blanket consent to search the contents of an electronic storage device, the government could argue that the client has implicitly waived any privilege that might otherwise exist. [32] Refusing to consent to the examination, on the other hand, may preserve the client's privilege, but government officials may nonetheless require the traveling client to make an unpalatable choice between consenting to the disclosure of privileged materials or seeing an expensive and important electronic device confiscated, at least for some period of time. The problem is particularly acute for a client who may not focus on the fact that her laptop may contain, for example, all of her e-mails—including e-mails to and from her lawyer.

Attorneys who carry privileged information during international travel also have to consider the implications of the government's claimed search authority. Attorneys have an ethical obligation to maintain client confidences. For instance, the American Bar Association's Model Rules of Professional Conduct provide that ''an attorney shall not reveal information relating to the representation of a client unless the client gives informed consent . . . .''[33] Though the ABA rule contains an exception for disclosures ''required by law,'' an attorney who takes the position that disclosure is required would essentially be agreeing to the government's claim of unfettered authority to conduct warrantless searches of otherwise privileged materials. Attorneys thus should consider themselves under an obligation to resist any government efforts to search electronic storage devices containing privileged material, unless the government takes adequate steps to ensure that it will not review any privileged material.

In order to provide the maximum protection for privileged materials, attorneys and clients should consider implementing safeguards to protect such materials in the event the government attempts to search a computer or other electronic storage device. First, because attorneys and clients are expected to guard privileged information carefully, they should minimize the amount of such information in their possession when traveling under circumstances where disclosure may be unavoidable. For those who need access to data at their destination, consider, if practicable, carrying a computer with a hard drive that contains only the information needed to access the data remotely over the Internet or over corporate networks at the individual's destination. While there may be some concerns about the potential risk to information accessed through the Internet, technical measures such as virtual private networks are commercially available and widely used to limit this risk.

Where remote access is not a viable option, consider segregating privileged information and clearly labeling it as privileged; this may help prevent inadvertent disclosures and provide a basis for a motion to exclude evidence should the government seize the storage device and intentionally access privileged materials.[34]

Encrypting sensitive information may be another effective way of preserving its integrity during international travel. However, travelers should be aware that U.S. export control restrictions may limit or prevent them from carrying encrypted data to certain locations.[35] In addition, apart from whether the government ultimately prevails in court on a motion to compel the passenger to disclose her encryption password, refusing to provide that password at the border may lead to a difficult choice of leaving the laptop in the government's custody or delaying one's plans to enter or leave the country.

And where it appears that the government is going to confiscate a computer with or without a party's consent, attorneys and clients should clearly indicate that the seized electronic device contains privileged material and that the government is not authorized to review those materials.[36]

---

[31] *In re Sealed Case*, 877 F.2d 976, 980 (D.C. Cir. 1989).

[32] *See, e.g., United States v. Workman*, 138 F.3d 1261, 1263 (8th Cir. 1998) (''Voluntary disclosure of attorney client communications expressly waives the privilege . . . .''); *United States v. Bernard*, 877 F.2d 1463, 1465 (10th Cir. 1989) (''Any voluntary disclosure by the client is inconsistent with the attorney-client relationship and waives the privilege.''); *Federal Election Comm'n v. Christian Coalition*, 178 F.R.D. 61, 71-72 (E.D. Va. 1998) (''Under the common law of attorney-client privilege, the parties privy to the communication must zealously and carefully guard against disclosure to third parties. Courts in this area take almost a strict liability approach to third party disclosure. If the information ends up in the hands of a third party, courts don't want to hear how it got there.''), *order aff'd in part, modified in part*, 178 F.R.D. 456 (E.D. Va. 1998).

[33] ABA Model Rules of Professional Conduct, Rule 1.6.

[34] *Cf. United States v. Valencia-Trujillo*, No. 8:02-CR-329-T-17EAJ, 2006 WL 1793547, at *9 (M.D. Fla. June 26, 2006) (concluding that there was no Fourth Amendment violation where customs agents seized documents belonging to defense investigator during border stop; because investigator asserted privilege, documents seized were sealed pending review, and government returned documents to defense without opening sealed documents).

[35] With the exception of Cuba, Iran, North Korea, Sudan and Syria, it is generally legal to carry abroad for temporary use a laptop with commercially available encryption, provided that the laptop is kept under one's effective control at all times and returned to the United States. Some license exceptions are available even for these five countries. The export regulations are complicated and should be consulted if there is any concern in this regard. 15 C.F.R. § 730 et seq.

[36] Department of Justice policy requires that agents searching a computer that contains legally privileged materials use a third party to separate privileged documents from unprivileged ones. U.S. Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, § II.B.7.b. (2002), online at http://op.bna.com/pl.nsf/r?Open=byul-7c2rfx.

Though Customs and Border Protection (CPB) falls within the purview of the Department of Homeland Security, courts

4. *What Options Do Travelers Have When Confronted with a Government Request to Search a Laptop Computer or Other Electronic Storage Device?*

While the uncertain scope of governmental authority in this area should cause passengers to exercise caution when traveling with electronic storage devices, travelers are unlikely to stop carrying these devices. What options, then, does an international traveler have when the government pulls her out of line and asks to view the contents of her computer?

Unfortunately, there are only a few realistic options should this situation arise. First, the traveler can consent to the government's request. This option is most likely to shorten the encounter, which explains why many people accede to the government's wishes. Yet the presence of even an utterly innocuous file name such as ''Blueprints'' may result in your computer being seized for further inspection.[37] Combine that possibility with the potential disclosure of sensitive, if not privileged, information, and the option of least resistance may be less palatable.

Refusing to consent to the search of the computer is not without drawbacks. Anecdotal evidence suggests that American citizens who refuse to grant the government consent will be allowed to return to the country, but that the electronic storage devices that are the subject of the search requests will be seized, copied, and then mailed back to the traveler.[38] In such circumstances, a traveler may legitimately wonder whether her privileged materials are better off being subjected to a cursory glance (if the inspection ends there) as opposed to having them copied and retained by government officials. Though the compelled production of an otherwise privileged communication will not waive the attorney-client privilege, [39] that is small comfort to the person whose confidential communications are seized and retained by the government.

There are also, of course, other practical considerations flowing from the types of information stored on the electronic storage device. What if the computer contains important medical information? Or what if it contains valuable proprietary information critical to the success of a business venture? Will refusing consent lead to the seizure and indefinite retention of that important information by government officials? One member of the Association of Corporate Travel Executives (ACTE) reported that her laptop computer was seized and that it had not been returned over a year later.[40] There have also been reports of information being deleted from electronic storage devices seized during border searches.[41]

Though the increased public attention to the government's search policies should cast more light on the government's activities, international travelers need to exercise a great deal of caution when carrying sensitive materials. As is so often the case, the safest option may be a healthy dose of prevention, utilizing some of the measures discussed with respect to the preservation of privileged materials. That may ultimately be the only way for an international traveler to conduct necessary business without permitting the government to intrude into an individual's private affairs.

Ronald Lee is a partner in the Washington office of Arnold & Porter LLP, practicing in national security, cybersecurity, and technology law and policy. He was formerly Associate Deputy Attorney General with the U.S. Department of Justice, where he served as director of the Executive Office of National Security. Lee can be reached at (202) 942-5380 or Ronald.Lee@aporter.com. Robert Litt is a partner in the Washington office of Arnold & Porter LLP, concentrating in information security and white collar criminal defense. Litt was formally principal Associate Deputy Attorney General in the U.S. Department of Justice, where he also served as Deputy Assistant Attorney General in the Criminal Division. He can be reached at (202) 942-6380 or Robert.Litt@aporter.com. Stephen Marsh is an associate in the Washington office of Arnold & Porter LLP, practicing in white collar criminal defense and general civil litigation. He was formerly an Assistant U.S. Attorney. He can be reached at (202) 942-5232 or Stephen.Marsh@aporter.com.

generally disapprove of law enforcement agents who knowingly review privileged materials where an express claim of privilege has been asserted. *See, e.g., United States v. Wilson*, 864 F.2d 1219, 1223 (5th Cir. 1989) (describing customs agents' knowing seizure of privileged materials, in context of abuse of process appeal, as ''outrageous and reprehensible . . . .'').

[37] *See* Joe Sharkey, *To Do List: Rename Laptop Files 'Grandma's Favorite Recipes,'* N.Y. TIMES, Nov. 7, 2006, at C6 (describing incident where passenger's computer was searched and then seized after agent noticed file named ''Blueprints.'').

[38] Joe Sharkey, *At U.S. Borders, Laptops Have No Right to Privacy*, N.Y. TIMES, Oct. 24, 2006, at C8.

[39] *Cf. Transamerica Computer Corp. v. Int'l Bus. Machines,* 573 F.2d 646, 651 (9th Cir. 1978) (recognizing that attorney-client privilege is not waived where disclosure is compelled).

[40] Sharkey, supra, note 38.

[41] *E.g.*, Nakashima, *supra* note 2.

  PVLR ISSN 1538-3423