

## CLIENT ADVISORY

## WORKING ON THE FLIGHT? HOW INTERNATIONAL TRAVEL CAN RESULT IN GOVERNMENT OFFICIALS EXAMINING YOUR ELECTRONIC DATA

Experienced international business travelers are familiar with the inspection of luggage by customs officials when returning to the United States. But they may not know that the United States Government claims the authority, as part of its power to search persons entering the country, to review the contents of laptops, Blackberries®, PDAs, cellphones, and other electronic storage devices. And where that content is password protected, the Government maintains that it has the power to compel an individual to provide the password so that encrypted materials can be reviewed.

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.<sup>1</sup>

Federal law expressly authorizes customs officials to detain and search individuals coming into the United States from foreign countries.<sup>2</sup> And the Fourth Amendment does not prohibit customs officials 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.<sup>3</sup> Border searches are deemed to be reasonable “simply by virtue of the fact that they occur at the border,”<sup>4</sup> where the government has a compelling interest in regulating the collection of duties and preventing contraband from entering into the country.<sup>5</sup> International airport terminals are considered the “functional equivalent” of borders,<sup>6</sup>

FEBRUARY 2008

**Washington, DC**  
+1 202.942.5000

**New York**  
+1 212.715.1000

**London**  
+44 (0)20 7786 6100

**Brussels**  
+32 (0)2 517 6600

**Los Angeles**  
+1 213.243.4000

**San Francisco**  
+1 415.356.3000

**Northern Virginia**  
+1 703.720.7000

**Denver**  
+1 303.863.1000

<sup>1</sup> *E.g.*, Ellen Nakashima, *Clarity Sought on Electronics Searches*, WASHINGTON POST, Feb. 7, 2008, at A01; 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).

<sup>2</sup> See 19 USC. § 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).

<sup>3</sup> *United States v. Montoya de Hernandez*, 473 US 531, 538, 105 S. Ct. 3304, 3309 (1985).

<sup>4</sup> *United States v. Ramsey*, 431 US 606, 616, 97 S. Ct. 1972, 1978 (1977).

<sup>5</sup> *Montoya de Hernandez*, 473 US at 537, 105 S. Ct. 3304, 3308 (1985).

<sup>6</sup> *United States v. Okafor*, 285 F.3d 842, 845 (9th Cir. 2002).

*This summary is intended to be a general summary of the law and does not constitute legal advice. You should consult with competent counsel to determine applicable legal requirements in a specific fact situation.*

**arnoldporter.com**

so “passengers deplaning from an international flight are subject to routine border searches.”<sup>7</sup> The same rule likely applies to passengers leaving the country on an international flight.<sup>8</sup>

Courts have not provided definitive guidance as to what constitutes a “routine” border search. The Supreme Court has hinted that *any* search at the border may be considered “routine” if it does not involve an invasive search of an individual and does not involve the physical destruction or alteration of the evidence being searched.<sup>9</sup> The mere fact that a search may take some time does not transform it into a “non-routine” search that would require a heightened standard of suspicion.<sup>10</sup>

While border search authority has traditionally allowed agents to search luggage thoroughly, a search of electronic devices such as computers or PDAs is far more intrusive. Electronic storage devices contain vast amounts of information, and because that information frequently can be sensitive or personal or even privileged, reviewing the contents of an electronic storage device seems less like a “routine” border search than riffling through a traveler’s clothes. A federal district court in California, for instance, granted a defendant’s motion to suppress computer evidence that was obtained as part of a border search where there was no reasonable suspicion of criminal activity. The court premised its ruling on the fact that laptops 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.”<sup>11</sup>

However, most courts that have considered the issue have taken a different view, implicitly reasoning that because computers and other electronic storage devices may contain contraband (such as child pornography), examining the contents of those devices is a necessary part of the government’s efforts to control the border.<sup>12</sup>

In some instances, however, the government cannot search a computer or other electronic storage device because its contents have been encrypted, and are therefore accessible only by a password known to the person in possession of the device. In one recent federal case,<sup>13</sup> 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 clearly indicated the likely presence of child pornography on the computer. However, when the case agent attempted to open the files to examine the contents, he was unable to do so because the files had been encrypted.

The government asked the court to compel the defendant to produce the password, but a federal magistrate judge held that compelled production of the password would violate the defendant’s Fifth Amendment rights. Some commentators have expressed disagreement with this decision;<sup>14</sup> whether other courts will follow it and protect an individual’s password

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

8 *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).

9 *United States v. Flores-Montano*, 541 US 149, 152, 155, 124 S. Ct. 1582, 1585, 1587 (2004).

10 *Id.* at 155, n.3, 124 S. Ct. at 1585 (concluding that delays of up to one or two hours at an international border are to be expected and do not provide grounds for a Fourth Amendment challenge to an otherwise valid border search).

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

12 *See, e.g., United States v. Ickes*, 393 F.3d 501, 506-07 (4th Cir. 2005) (concluding that customs officials did not violate defendant’s Fourth Amendment rights by examining contents of computer and related disks as part of a border search); *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); *cf. Romm*, 455 F.3d at 996-97 (upholding forensic analysis of computer evidence seized without a warrant because evidence was lawfully examined as part of a border search, though refusing to consider whether examination was “routine” because question had not been addressed below).

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

14 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*, February 4, 2008, <http://writ.news.findlaw.com/colb/20080204.html>

from compelled government disclosure remains to be seen. Moreover, as a practical matter, if a traveler declines to provide the password, customs officials can conduct an extensive “routine” search that may delay and inconvenience the traveler.

### SUGGESTED ACTIONS WHEN TRAVELING WITH ELECTRONIC STORAGE DEVICES

In light of the existing uncertainty in this area of the law, international travelers should exercise caution before traveling abroad with a computer, Blackberry®, iPod®, PDA, cellphone, thumb-drive, or any other type of electronic storage device that might contain sensitive, personal or proprietary information, and companies whose employees frequently travel internationally should consider establishing policies in that regard.

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.

Any policy adopted should specifically address traveling with information which might be considered privileged. Blanket consent to the examination of the contents of an electronic storage device could be deemed a waiver of any applicable privilege.<sup>15</sup> Refusing to consent to the examination, on the other hand, may preserve the privilege,<sup>16</sup> but government officials may nonetheless require an international traveler to make an unpalatable choice between consenting to the disclosure of privileged materials or forfeiting the right to

travel with those items.

If travelers must carry sensitive electronic information while traveling abroad, they should take steps to protect that information from unintended disclosure. Segregating sensitive or privileged information and clearly labeling it may help prevent inadvertent disclosures and provide a basis for limiting government searches.<sup>17</sup> Encrypting sensitive information may be another effective way of preserving the integrity of that information. However, travelers should be aware that US export control restrictions may limit or prevent them from carrying encrypted data to certain locations.<sup>18</sup>

---

*We hope you find this summary helpful. If you would like more information about the implications of traveling abroad with electronic storage devices, please feel free to contact your Arnold & Porter attorney or*

**Robert Litt**  
+1 202.942.6380  
Robert.Litt@aporter.com

**Ronald Lee**  
+1 202.942.5380  
Ronald.Lee@aporter.com

**Stephen Marsh**  
+1 202.942.5232  
Stephen.Marsh@aporter.com

<sup>15</sup> 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.”).

<sup>16</sup> 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).

<sup>17</sup> 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). 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. US Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, § II.B.7.b. (2002), online at [http://www.cybercrime.gov/s&smanual2002.htm#\\_IIB7b](http://www.cybercrime.gov/s&smanual2002.htm#_IIB7b).

<sup>18</sup> 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 US. 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.