

Department of Homeland Security Policy on Laptop Searches at the Border: An Analysis

September 9, 2008

On July 16, U.S. Customs and Border Protection (CBP), an agency within the Department of Homeland Security (DHS), published policy guidance with respect to its authority to conduct border searches of information contained in documents and electronic devices. Specifically, the policy guidance “sets forth the legal and policy guidelines within which [CBP] officers may search, review, retain, and share certain information” that is transported across the U.S. border. Border searches of information and documents are conducted absent probable cause or warrants and may be conducted on any individual seeking to enter the United States regardless of citizenship or nationality. A recent court decision issued by the Ninth Circuit Court of Appeals has upheld CBP’s authority to conduct searches of electronic information without reasonable suspicion. *United States v. Arnold*, 523 F.3d 941 (9th Cir. 2008) (holding that customs officers may examine the electronic contents of a passenger’s laptop or other personal electronic storage devices at the border without reasonable suspicion).

CBP thus far has been unwilling to modify or limit its authority to conduct searches of information contained in documents and electronic devices. The issue has garnered much attention from private-sector organizations and activist groups. On June 25, the U.S. Senate Committee on the Judiciary Subcommittee on the Constitution, Civil Rights, and Property Rights held a hearing on “Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel.” However, in light of judicial precedent that supports CBP’s activities, this issue is likely to remain a point of contention for the foreseeable future.

Below is a brief overview of search and seizure at the U.S. border, CBP’s current scope of authority, and recommendations on how to protect confidential data when returning to the United States after international travel.

Search and Seizure at the U.S. Border

The Fourth Amendment to the United States Constitution prohibits the government from conducting unreasonable searches and seizures. While in most cases searches and seizures must be conducted pursuant to a finding of probable cause and issuance of a warrant, the U.S. Supreme Court has carved a “border search exception,” which allows searches of individuals and property entering the United States without probable cause or a warrant. *United States v. Ramsey*, 431 U.S. 606 (1977). This exception is based on the inherent authority of the government to control persons and objects entering its territory. Moreover, the Court determined that individuals possess a diminished expectation of privacy at the border.

As a result of *Ramsey*, individuals and property entering the United States may be subject to warrantless and random searches and seizures, absent probable cause, at the border; however, such searches and seizures must be “routine” in order to be covered by the border search exception. “Routine” searches include searches of cargo and luggage, and opening of sealed packages. Nonroutine searches typically involve invasive physical searches; for example, a search of a drug smuggler who has swallowed bags of cocaine. Nonroutine searches require reasonable suspicion prior to conducting the search. *United States v. Montoya de Hernandez*, 473 U.S. 531 (1985).

Laptop Searches Are Generally Considered to Be Routine Border Searches

Although the U.S. Supreme Court has yet to address the question of border searches of electronic materials, several lower courts have concluded that searches of laptops fall within the realm of routine searches at the border and therefore do not require reasonable suspicion. See, e.g., *Arnold*, 523 F.3d 941; *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005); *United States v. Bunty*, Crim. No. 07-641, 2008 WL 2371211 (E.D. Pa. June 10, 2008); *United States v. Roberts*, 86 F. Supp. 2d 678 (S.D. Tex. 2000). In the absence of conflicting lower court determinations, it is unlikely that the U.S. Supreme Court will intercede at this point.

In addition, in light of judicial precedent recognizing an inherent right of the government to protect its borders and the law enforcement responsibilities of CBP, routine border searches of laptops will likely be exempt from Privacy Act protection. The European Union has a convention on privacy and the protection of data; however, no corresponding international conventions apply to individuals seeking admission to the United States.

How This Affects You

According to the July 16 CBP guidance, officers may detain documents and electronic devices, or copies thereof, for a reasonable period of time to perform a search. Absent probable cause, CBP officers may not seize the documents or information, and any copies must be destroyed after review. CBP officers are bound by the Trade Secrets Act, which prohibits federal employees from disclosing, without lawful authority, business confidential information acquired as part of their official duties. The guidance instructs CBP officers to take all reasonable measures to protect commercial and business information.

In light of the volume of information stored on laptops as well as the sensitive nature of the data, we recommend that all international travelers take the following precautions:

1. Clearly mark sensitive information as "confidential." The following labels are appropriate for use:
 - Attorney-Client Work Product
 - Privileged and Confidential Attorney-Client Communication
 - Highly Sensitive Confidential Material
 - Confidential Medical Information

According to the July 16 policy guidance, CBP is required to request permission from the Office of General Counsel prior to viewing certain confidential information.

2. Any sensitive documents should be subject to password protection and placed in folders. The folders as well can be subject to password protection. While a CBP officer could certainly request the password from the business traveler, this provides notice as to what documents are about to be viewed, and the business traveler can request that the CBP officer check with CBP Office of General Counsel before proceeding.
3. Any data that cannot or should not be exposed to the public should be downloaded to a data stick and taken off the laptop's hard drive. While CBP could view the data stick, this measure will likely afford an additional layer of protection.
4. Clean email systems prior to travel and ensure that any confidential emails are placed into password-protected folders.

Morgan, Lewis & Bockius will continue to monitor the situation and will update you with any new information. If you have any questions about any of the issues raised in this Morgan Lewis Immigration Alert, please contact: Title

San Francisco

A. James Vázquez-Azpiri 415.442.1343
Lance Nagel 415.442.1345

ajvazquez@morganlewis.com
lnagel@morganlewis.com

Washington, D.C.

Eleanor Pelta 202.739.5050
Eric S. Bord 202.739.6040

epelta@morganlewis.com
ebord@morganlewis.com

About Morgan, Lewis & Bockius LLP

Morgan Lewis is a global law firm with more than 1,400 lawyers in 22 offices located in Beijing, Boston, Brussels, Chicago, Dallas, Frankfurt, Harrisburg, Houston, Irvine, London, Los Angeles, Miami, Minneapolis, New York, Palo Alto, Paris, Philadelphia, Pittsburgh, Princeton, San Francisco, Tokyo, and Washington, D.C. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.

This LawFlash is provided as a general informational service to clients and friends of Morgan, Lewis & Bockius LLP. It should not be construed as, and does not constitute, legal advice on any specific matter, nor does this message create an attorney-client relationship. These materials may be considered **Attorney Advertising** in some states. Please note that the prior results discussed in the material do not guarantee similar outcomes.

© 2008 Morgan, Lewis & Bockius LLP. All Rights Reserved.

