McKenna Long & Aldridge LLP
Attorneys at Law

STAY AHEAD OF THE CURVE

International Law Report
March 2008

Recent Trends Suggest Travelers Going Abroad Should Do So With A "Clean" Laptop

CONTACTS

If you would like more information, please contact any of the McKenna Long & Aldridge attorneys or public policy advisors with whom you regularly work. You may also contact:

John R. Liebman
213.243.6140

Kevin J. Lombardo
213.243.6198

Virginia M. Gomez
213.243.6156

Travelers entering and leaving the United States with laptops historically need only worry about those laptops containing technical data controlled by the International Traffic and Arms Regulations (ITAR) or the Export Administration Regulations (EAR). International travelers with laptops are or should be generally aware that they must either secure the proper export license, carry documentation demonstrating that they qualify for an exemption or exception to an otherwise applicable license requirement, or simply ensure that their laptops do not contain any technical data.[1]

Recently, however, agents of the United States Customs and Border Protection (USCBP) have made all travelers, not just those who frequently carry technical data and are accustomed to complying with U.S. export controls, think twice about exiting or entering the United States with *any* sensitive data in any format. In an apparent attempt to identify information linked to terrorism, narcotics smuggling and other possible criminal activity, USCBP agents have conducted searches, and in some cases seizures, of devices that contain electronic data, including laptops, cellular phones, BlackBerries® and other personal digital assistant (PDA) devices.

Government searches of data contained on electronic devices, primarily laptops, raise several potential concerns. First, these searches threaten the integrity of confidential data. It is unclear what procedures apply to customs agents' use and/or protection of the data searched/seized. As a result, all types of sensitive data risk exposure. Border protection agents could easily view, or possibly seize, the following types of sensitive data from travelers:

- Business/proprietary data or trade secrets;
- Customer or client files (which may include business and/or proprietary data) and attorney-client privileged information;
- Personal data (websites visited, emails, etc.).

In addition, recent USCBP actions suggest that the U.S. Government believes that constitutional protections against illegal search and seizure do not fully regulate these searches on the grounds that inbound travelers who have not cleared customs are not "officially" in the country for Fourth Amendment protection purposes. To address this issue, several lawsuits were recently filed to determine what legal limitations there are on the USCBP's ability to conduct these electronic device searches. These cases include *inter alia* a recent complaint filed by the Electronic Frontier Foundation (EFF) seeking injunctive relief with respect to an unanswered Freedom of Information Act (FOIA) request to obtain USCBP's policies and procedures on the questioning, search and inspection of travelers entering or returning to U.S. ports of entry; and *In re Boucher*, 2007 WL 4246473 (D. Vt. 2007), wherein the court held that the

defendant did not have to provide a password to the government in order for the government to access encrypted files on his laptop on Fifth Amendment right against self-incrimination grounds.

All international travelers–both U.S. and foreign–should be aware that they may be forced to disclose any information that resides on their laptops or other electronic devices at U.S. ports of entry. Until there is some definitive resolution regarding the scope of the USBCP's search and seizure power, travelers may want to carry a "clean" laptop (*i.e.,* without any sensitive data), and use alternative means to access necessary data from their destination points outside the U.S., such as arranging to log onto a secure company server from a remote access point.

---

[1] Laptops themselves may require export licenses if the itinerary includes any of the Commerce or Treasury-sanctioned countries, viz Cuba, North Korea, Syria, Sudan or Iran.

About Us

McKenna Long & Aldridge LLP is an international law firm composed of lawyers and public-policy advisors with offices in Albany, Atlanta, Brussels, Denver, Los Angeles, New York, Philadelphia, San Diego, San Francisco, and Washington, DC. The firm provides business solutions in the areas of corporate law, government contracts, intellectual property and technology, complex litigation, public policy and regulatory affairs, international law, real estate, environmental, energy, and finance.

Subscription Info

If you would like others to receive future mailings of the International Law Report, please email their contact information to us at information@mckennalong.com

If you would like to be removed from the International Law Report mailing list, please email information@mckennalong.com