# Are You Ready to Have Your Laptop Searched or Seized at a U.S. Border?

Jul 01 2008

Posted By: Mark F. Foley

Practice Area: Information Technology, Data Privacy and Security

Many business travelers have been surprised to learn from recent newspaper articles that their laptops and other electronic files may be searched or even seized by U.S. Customs officials when returning to the U.S. from an international journey. Why is this so? How much risk does a legitimate business traveler face? What should international business travelers do to prepare for a potential search or seizure?

We have all become accustomed to taking our business laptops, phones, Personal Digital Assistants, digital cameras and memory sticks on international trips. We do this as a matter of course, whether it's a pure business trip or a family vacation when we need to keep business projects moving or just need to keep in touch with our colleagues and clients. Often, this means that thousands of emails and attachments, personal and business photographs, Adobe pdf files, spreadsheets, memoranda, and telephone logs are with us as we leave the country. A recent decision out of the Ninth Circuit Court of Appeals makes clear that all such information can be searched and seized when a traveler returns to the United States, even if there is no reasonable basis for believing that the traveler has engaged in or is planning to engage in any unlawful conduct.

The general response to this decision has been incredulity. Don't I have a right of privacy? Doesn't the Constitution protect me against unreasonable searches and seizures? Doesn't the government need a warrant based on probable cause before seizing my personal and business files? The simple answer is "no."

Contrary to popular belief, there is no general "right of privacy" in the United States. No such right is enumerated in the Constitution or Bill of Rights, although some provisions in the Bill of Rights recognize specific privacy interests. Several U.S. Supreme Court cases have also recognized broader privacy interests based on the "penumbra's" of the enumerated rights. Although some State constitutions recognize a general right of privacy, no federal statute creates such a generalized right, and any state law based right would be subject to the Supremacy Clause of the U.S. Constitution, which gives federal law supremacy over any conflicting State law.

So what are our rights, really? The Fourth Amendment to the U.S. Constitution states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated..." In the context of domestic searches, this has been interpreted to mean that in most cases there must be a warrant issued after demonstrating to a judicial officer that there is probable cause that the target of an intended search has committed or is about to commit a crime or has evidence relating to a crime.

But the definition of what is "unreasonable" is different in the international arena. The Supreme Court has recognized that, as a sovereign, the U.S. has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity through control of its borders. As a result, the U.S. government is entitled to search the baggageof arriving international travelers and to require whoever seeks entry to establish the right to enter and to bring into the country whatever he may carry. Generally, "searches made at the border...are reasonable simply by virtue of the fact that they occur at the border..." *U.S. v. Ramsey*, 431 U.S. 606, 616 (1977). The luggage carried by a traveler entering the country may be searched at random by a customs officer, no matter how great the traveler's desire to conceal the contents may be, whether the traveler is an itinerant who carries a tooth brush and a few articles of clothing in a paper bag or a sophisticated executive with a locked attaché case and a laptop computer. *United States v. Ross*, 456 U.S. 798, 823 (1982).

There are some limits. The interests in human dignity and privacy which the Fourth Amendment protects forbid any intrusion beyond the body's surface on the mere chance that desired evidence might be obtained. The Supreme Court has also held open the possibility "that some searches of property are so destructive as to require" particularized suspicion. But searches of a laptop or memory stick are not inherently destructive. The Supreme Court has also rejected creating a balancing test based on distinctions between "routine" and "non-routine" searches.

These issues were addressed by the 9th Circuit Court of Appeals in an April 2008 decision in *U.S. v. Arnold*. Arnold returned to the U.S. from a trip to the Philippines. A Customs officer at the Los Angeles airport selected Arnold for special attention at the border, demanding that he boot up his laptop computer. The Customs agents then looked at two folders and found images that they believed constituted illegal child pornography. Arnold's computer was confiscated and he was indicted. Arnold argued that the search of his computer was unreasonable and the evidence it uncovered should be suppressed. The Ninth Circuit disagreed, holding that neither the amount of information contained on the laptop, its analogy to a "home," general privacy expectations, or First Amendment rights in the communications held on the laptop, protected Arnold from a random search.

What should you do in response to this reality? First, alert your traveling executives to the risks involved. Have them think about how to minimize the amount of sensitive information they take or acquire overseas. Rather than copying large files before heading overseas, explore whether information can be accessed when needed through a virtual private network, without it actually be saved to the laptop. Second, make sure your executives know their rights and responsibilities at the border and what to do if they are asked to turn on or turn over a laptop or stored electronic files. Who should be advised that materials were searched or seized. If materials have been seized, who should be contacted to get them back? Who should make that contact? Third, make sure that all critical information that may be on a laptop or removable media is backed up to your corporate systems. If information exists only on an executive's laptop, seizure of the device could be debilitating. Fourth, contact your U.S. Senators and Congressmen to tell them that you think the current rules are too intrusive and that legitimate businessmen should have more protection.

---