Privacy Alert

Gov't Rummaging Through Your Laptop's Contents? No Problem If You're Re-Entering USA, Says Ninth Circuit

MITCHELL ZIMMERMAN

FENWICK & WEST LLP

You've gotten used to being asked to turn on your laptop as you go through airport security so the authorities can confirm it's really a computer and not a bomb. But you may not expect, on returning home from abroad, to have U.S. Customs demand your computer password so they can scrutinize your computer's contents, make a mirror image of your entire hard drive, or "temporarily" seize your laptop.

Start expecting it. Customs has been making such demands and engaging in such invasive searches and seizures. And last week the Ninth Circuit Court of Appeals held that the government has unfettered discretion to do so, with no requirement of reasonable suspicion to think you or your computer are implicated in any criminal activity. *United States v. Arnold,* No. 06-50581 (9th Cir. April 21, 2008). In *Arnold,* the officer booted up the defendant's computer and opened up folders called "Kodak Pictures" and "Kodak Memories." On seeing two images of nude women, the officer called in agents of Homeland Security to question Arnold and further search his computer. After finding numerous images of alleged child pornography, the officials seized the laptop, and eventually Arnold was criminally charged. The district court granted Arnold's motion to suppress the evidence on the ground that the search was not justified by any reasonable suspicion. The Ninth Circuit reversed. (Arnold reportedly plans to petition for rehearing *en banc*.)

The Ninth Circuit's logic and holding. The court reasoned that the Fourth Amendment's protection against unreasonable searches and seizures simply does not apply to searches at the border (or at airports of entry). As the Supreme Court has held, "The authority of the United States to search the baggage of arriving international travelers is based on its inherent sovereign authority to protect its territorial integrity." It follows, the Supreme Court has stated, that as a general matter "searches made at the border ... are reasonable simply by virtue of the fact that they occur at the border." Customs therefore has discretion to search luggage and the goods of incoming travelers for any reason or no reason, without any showing of reasonable suspicion. It makes no difference, concluded the Ninth Circuit, that a searched "container" holds vast amounts of personal or confidential business information: "Arnold has failed to distinguish how the search of his laptop and its electronic contents is logically any different from the suspicionless border searches of travelers' luggage that the Supreme Court and we have allowed."

The court dismissed concerns regarding any privacy or First Amendment interests. The holding:

"[R]easonable suspicion [of any crime or wrongdoing] is not needed for customs officials to search a laptop or other personal electronic storage devices at the border."

Implications for law-abiding business people. The power to engage in such searches and seizures without constitutional justification has disturbing implications for business. And while Customs asserts that its officers "are trained to protect confidential information," it is difficult to know what this means in practice. Consider these scenarios.

- Perhaps you are the CEO of a public company, whose laptop contains confidential notes on a planned acquisition or nonpublic information on earnings. A Customs Officer may access, copy and scrutinize those files, or turn them over to other unknown government employees or agencies, leaving you to wonder whether your seemingly secret information will be leaked or might generate what looks like insider trading.
- Or perhaps your computer contains an image of a new consumer electronics product, whose configuration is being kept ultra-hush until the product is released. Now you may need to worry about whether a government employee may gossip about what you consider a carefully guarded trade secret. This could result in premature media reports, and possibly a breach of statutory or contractual confidentiality obligations.
- Or perhaps you are the Chief Information Officer of an internet enterprise, and your computer holds a copy of a database of customer information, including personally identifying information. If the government seizes your computer or makes a mirror image of your hard drive, and the copy is subject to no apparent legal constraint, must you notify your customers of a security breach?
- Or perhaps you are in-house counsel, and your laptop holds memoranda on your company's regulatory

compliance. Bear in mind, then, that Customs can make a copy of any attorney-client material or work product that is on your computer. It is not clear whether anything seriously restrains them from reading and forwarding it to any government agency that a customs officer thinks may find it of interest.

On the other hand, if you actually are an al Qaeda terrorist, you will not likely find yourself seriously inconvenienced by these practices. Insofar as a terrorist's plans might require written materials, he can simply email them to himself and travel without a computer, purchasing a new one after arrival in the United States.

What's to be done. How much trouble you want to take to avoid these possible scenarios turns on several considerations: how confidential and proprietary you consider the material on your laptop to be; how sensitive you are to intrusions into your intellectual property, communications and business affairs (not to mention any personal matter that may also be on your computer); and how willing you are to trust that government officials and employees will not misuse what they seize or negligently disclose confidential information.

- At a minimum, consider removing anything that constitutes a significant trade secret and other truly confidential matter from your computer before traveling, and storing such materials on a stay-at-home drive or backup. Keep in mind, however, that something more than routine file deletion may be required to keep such materials from being reconstructed in the event your laptop is seized or the entire hard drive copied.
- If you are more deeply concerned, consider traveling with a computer with a fresh hard drive or lease a computer on arrival, and either email to yourself any materials that will be needed when you are abroad or access those items via the internet (i.e., on an .ftp site or extranet). Before returning, try to effectively delete such materials. You may consider storing on a flash memory stick (or USB drive) anything you download and work on while overseas, and physically destroying the device after emailing its contents to yourself or uploading to a secure site prior to your return. In this event, you may need to redirect your browser's temp files to the USB drive, something you should consult with your IT department about. Bear in mind, though, that if your computer is seized, or a mirror copy is made of its hard drive, you cannot be confident that you will have deleted confidential information in a manner that defies a determined effort at restoration. Similarly, a forensic level analysis of the computer could negate the effects of attempting to work exclusively on the USB device.
- The same legal principles appear to apply to handheld email devices and cell phones and to any email or text messages found on them.
- Full-disk or selected file encryption could provide further protection, and is in any event recommended for business laptops containing confidential or proprietary information. But difficult issues would be posed when government officials demand passwords, and the outcome is not clear if travelers decline to provide them.
- For further thoughts on what-to-do, see Declan McCullagh's "Security guide to customs-proofing your laptop," http://www.news.com/8301-13578_3-9892897-38.html?tag=nefd.lede, or "How Does Bruce Schneier Protect His Laptop Data? With His Fists – and PGP," http://www.schneier.com/essay-199.html. And for more particularized counsel, and legal advice on these issues, contact Fenwick & West.

At the U.S. border, your laptop can and may be thoroughly searched even if you have done nothing to give rise to any reasonable suspicion of wrongdoing. Its contents can be viewed, seized and possibly forwarded to other government agencies. Rather than risk exposure of sensitive business and personal information when entering the country, plan ahead to avoid disclosing material that you are obligated to protect from unanticipated inspection and whose secrecy you may wish to preserve. Consider a combination of the above steps to avoid breaching fiduciary duties, clients' and customers' trust, and confidentiality and privacy obligations.

For further information on privacy issues and technology, please contact Mitchell Zimmerman, Co-Chair of the Firm's Privacy and Information Security Group, at 650.335.7228 (mzimmmerman@fenwick.com), Michael Blum, Co-Chair of the Firm's Privacy and Information Security Group, at 415.875.2468 (mblum@fenwick.com), or Matt Kesner, Chief Technology Officer for the Firm, at 650.428.4488 (mkesner@fenwick.com).