The Business Traveler's New Nightmare: Searches of Company Laptops and PDAs at the Border

Steptoe & Johnson LLP
1330 Connecticut Avenue, NW
Washington, DC 20036
Tel: 202.429.3000
Fax: 202.429.3902

750 Seventh Avenue
New York, NY 10019
Tel: 212.506.3900
Fax: 212.506.3950

115 South LaSalle Street
Suite 3100
Chicago, IL 60603
Tel: 312.577.1300
Fax: 312.577.1370

Collier Center
201 East Washington Street,
16th Floor
Phoenix, AZ 85004
Tel: 602.257.5200
Fax: 602.257.5299

633 West Fifth Street
Suite 700
Los Angeles, CA 90071
Tel: 213.439.9400
Fax: 213.439.9599

2121 Avenue of the Stars
Suite 2800
Los Angeles, CA 90067
Tel: 310.734.3200
Fax: 310.734.3300

Avenue Louise 240, Box 5
B–1050 Brussels
Belgium
Tel: +32 2 626 0500
Fax: +32 2 626 0510

Steptoe & Johnson
99 Gresham Street
London, EC2V 7NG
England
Tel: +44 20 7367 8000
Fax: +44 20 7367 8001

It's bad enough traveling these days, with long flight delays, security lines, baggage fees, and cramped seating. But if you're a corporate executive carrying sensitive company information, it can be a whole lot worse. U.S. Customs and Border Protection agents have reportedly been increasing their searches of traveler's laptops, PDA's, cellular telephones, and other mobile electronic devices at international airports and other border crossing. And they don't need any reason to suspect that a traveler is carrying contraband or doing anything wrong. They've also reportedly been seizing devices for extended periods as well. This means company trade secrets, proprietary data, and personal information are at risk not just from corporate spies, hackers, and identity thieves, but from government agents, too.

Searches At U.S. Border Crossings

The U.S. government has long maintained that it has the authority to search the belongings of persons coming across the border (including international air travelers at U.S. airports), without a search warrant or even any suspicion of a crime. It further asserts that this authority extends to electronic devices such as laptop computers, despite the First Amendment issues such searches might raise (if, for example, a border agent examines private correspondence stored on the device). And this authority applies not just to foreign nationals, but also to U.S. citizens returning home.

The U.S. Court of Appeals for the Ninth Circuit, in *United States v. Arnold* (April 21, 2008), recently upheld such suspicionless border searches. The Ninth Circuit relied on Supreme Court precedent establishing that the "Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border," while a person's "expectation of privacy [at the border] . . . is significantly less than that relating to one's home or office." The Ninth Circuit also reasoned that the search of a "piece of property … simply does not implicate the same 'dignity and privacy' concerns as 'highly intrusive searches of the person.'" The Fourth Circuit in 2005 reached a similar conclusion. The courts have left open the possibility, however, that searches that are destructive or conducted in a particularly offensive manner may require particularized suspicion of a crime.

Such border searches have recently drawn increased attention from the media and Congress. The Association of Corporate Travel Executives testified to Congress

The Business Traveler's New Nightmare: Searches of Company Laptops and PDAs at the Border

recently that in a poll it conducted of its members, 7 out of 100 respondents reported that they had had an electronic device seized by border agents.

In response to the increased attention, the Deputy Commissioner of U.S. Customs and Border Protection (CBP) on June 30, 2008 defended the government's practices in this area. He stated that searches of electronic devices were "central to keeping dangerous people and things from entering the country and harming the American people," citing terrorism, intellectual property rights violations, and child pornography as among the main concerns. The government has provided no details, however, on its policies or procedures concerning such issues as: When will it decide to conduct a search? When will it seize and retain an electronic device, and for how long? When will it copy information stored on a device? And how will it protect proprietary or confidential information.

What Should A Company Do?

Companies concerned about having their electronic devices searched or seized at the border, or having confidential information reviewed or copied, have several options (each with its own risks), including:

Not carrying laptops or other electronic devices across the U.S. border. This option has obvious costs, however, in terms of business efficiency.

Encrypting sensitive data stored on the device. It has been reported, however, that border agents have required travelers to provide the decryption key or password if they encounter encryption, and refused entry to non–U.S. persons (citizens or legal resident aliens) who have declined. It is not clear, however, what border agents would do if a U.S. person declines to provide an encryption key or password. One federal court has ruled that compelling a criminal suspect to enter his password in order to provide access to suspected child pornography on his laptop would violate his Fifth Amendment right against self–incrimination, though it is unclear whether this ruling will be sustained or how far it may extend.

Deleting sensitive data and "scrubbing" the device before crossing the border. Travelers can delete sensitive data from their devices before crossing the U.S. border and "scrub" the device to ensure that the data is not still retained in some part of the computer's memory. But such scrubbing must be performed by an experienced, technical professional in order to provide adequate assurance that the data cannot be found on the device.

The Business Traveler's New Nightmare: Searches of Company Laptops and PDAs at the Border

Emailing sensitive data rather than carrying it on a physical device. Travelers can email data to themselves and then download it when they get to their destination. If the data is accessed using the traveler's laptop, however, the data could be found in the laptop's memory unless the traveler is careful.

The Situation Abroad

The United States is not the only country where incoming travelers must be concerned about search or seizure of their laptops. Other countries also give border agents extensive authority to search and seize a traveler's belongings, including electronic devices. And security experts have raised well-founded concerns that some countries have made it a regular practice to search travelers' electronic devices and copy sensitive information.

Moreover, some countries strictly limit a person's ability to import or use encryption, including encryption on a traveler's laptop or other mobile device. To minimize the risks to their companies' proprietary data and to avoid having themselves or their devices seized, business travelers need to be aware of the panoply of different rules and practices that countries apply in this area.

Steptoe Can Help

Steptoe can help your company understand the risks to corporate data and take appropriate measures to protect your information. We regularly advise multinational corporations on data protection and security issues, including how to respond to government demands for information. With the assistance of a broad network of local counsel and other advisors, we also regularly counsel clients on compliance with international encryption and data protection regimes, including rules regarding encryption on mobile devices. We can help your company devise a comprehensive risk mitigation plan for international travel and cross-border information transfers, as well as provide last-minute advice on urgent questions. Before your company executives bring sensitive information or encrypted laptops across international borders, they need to know what they might be getting themselves, and the company, into. Steptoe can help.

★ ★ ★ ★ ★

Contact information: Michael Vatis, 212-506-3927, mvatis@steptoe.com