THE NEW YORK TIMES

October 24, 2006

On the Road

At U.S. Borders, Laptops Have No Right to Privacy

By JOE SHARKEY

A LOT of business travelers are walking around with laptops that contain private corporate information that their employers really do not want outsiders to see.

Until recently, their biggest concern was that someone might steal the laptop. But now there's a new worry — that the laptop will be seized or its contents scrutinized at United States customs and immigration checkpoints upon entering the United States from abroad.

Although much of the evidence for the confiscations remains anecdotal, it's a hot topic this week among more than 1,000 corporate travel managers and travel industry officials meeting in Barcelona at a conference of the Association of Corporate Travel Executives.

Last week, an informal survey by the association, which has about 2,500 members worldwide, indicated that almost 90 percent of its members were not aware that customs officials have the authority to scrutinize the contents of travelers' laptops and even confiscate laptops for a period of time, without giving a reason.

"One member who responded to our survey said she has been waiting for a year to get her laptop and its contents back," said Susan Gurley, the group's executive director. "She said it was randomly seized. And since she hasn't been arrested, I assume she was just a regular business traveler, not a criminal."

Appeals are under way in some cases, but the law is clear. "They don't need probable cause to perform these searches under the current law. They can do it without suspicion or without really revealing their motivations," said Tim Kane, a Washington lawyer who is researching the matter for corporate clients.

In some cases, random inspections of laptops have yielded evidence of possession of child pornography. Laptops may be scrutinized and subject to a "forensic analysis" under the so-called border search exemption, which allows searches of people entering the United States and their possessions "without probable cause, reasonable suspicion or a warrant," a federal court ruled in July. In that case, a man's laptop was found to have child pornography images on its hard drive.

No one is defending criminal possession of child pornography or even suggesting that the government has "nefarious" intent in conducting random searches of a traveler's laptop, Ms. Gurley said.

"But it appears from information we have that agents have a lot of discretion in doing these searches, and that there's a whole spectrum of reasons for doing them," she added.

The association is asking the government for better guidelines so corporate policies on traveling with proprietary information can be re-evaluated. It is also asking whether corporations need to cut back on proprietary data that travelers carry.

“We need to be able to better inform our business travelers what the processes are if their laptops and data are seized — what happens to it, how do you get it back,” Ms. Gurley said.

She added: “The issue is what happens to the proprietary business information that might be on a laptop. Is information copied? Is it returned? We understand that the U.S. government needs to protect its borders. But we want to have transparent information so business travelers know what to do. Should they leave business proprietary information at home?”

Besides the possibility for misuse of proprietary information, travel executives are also concerned that a seized computer, and the information it holds, is unavailable to its owner for a time. One remedy some companies are considering is telling travelers coming back into the country with sensitive information to encrypt it and e-mail it to themselves, which at least protects access to the data, if not its privacy.

In one recent case in California, a federal court went against current trends, ruling that laptop searches were a serious invasion of privacy. “People keep all sorts of personal information on computers,” the court ruling said, citing diaries, personal letters, financial records, lawyers’ confidential client information and reporters’ notes on confidential sources. That court ruled, in that specific case, that “the correct standard requires that any border search of the information stored on a person’s electronic storage device be based, at a minimum, on a reasonable suspicion.”

In its informal survey last week, the association also found that 87 percent of its members said they would be less likely to carry confidential business or personal information on international trips now that they were aware of how easily laptop contents could be searched.

“We are telling our members that they should prepare for the eventuality that this could happen and they have to think more about how they handle proprietary information,” Ms. Gurley said. “Potentially, this is going to have a real effect on how international business is conducted.”

E-mail: jsharkey@nytimes.com