

INTERNATIONAL
Herald Tribune

U.S. courts consider legality of laptop inspections

By Adam Liptak

Monday, January 7, 2008

A couple of years ago, Michael Arnold landed at the Los Angeles International Airport after a 20-hour flight from the Philippines. He had his laptop with him, and a customs officer took a look at what was on his hard drive. Clicking on folders called "Kodak pictures" and "Kodak memories," the officer found child pornography.

The search was not unusual: The government contends that it is perfectly free to inspect every laptop that enters the country, whether or not there is anything suspicious about the computer or its owner. Rummaging through a computer's hard drive, the government says, is no different from looking through a suitcase. One federal appeals court has agreed, and a second seems ready to follow suit.

There is one lonely voice on the other side. In 2006, Judge Dean Pregerson of U.S. District Court in Los Angeles suppressed the evidence against Arnold.

"Electronic storage devices function as an extension of our own memory," Pregerson wrote, in explaining why the government should not be allowed to inspect them without cause. "They are capable of storing our thoughts, ranging from the most whimsical to the most profound."

Computer hard drives, Pregerson continued, can include diaries, letters, medical information, financial records, trade secrets, attorney-client materials and information about reporters' "confidential sources and story leads."

But Pregerson's decision seems to be headed for reversal. The three judges who heard the arguments in October in the appeal of his decision seemed persuaded that a computer is just a container and deserves no special protection from searches at the border. The same information in hard-copy form, their questions suggested, would doubtless be subject to search.

The 4th U.S. Circuit Court of Appeals, in Richmond, Virginia, took that position in a 2005 decision. It upheld the conviction of John Ickes Jr., who crossed the Canadian border with a computer containing child pornography. A customs agent's suspicions were raised, the court's decision said, "after discovering a video camera containing a tape of a tennis match, which focused excessively on a young ball boy."

It is true that the government should have great leeway in searching physical objects at the border. But the law requires a little more - a "reasonable suspicion" - when the search is especially invasive, as when the human body is involved.

Searching a computer, said Jennifer Chacon, a law professor at the University of California, Davis, "is fairly intrusive." Like searches of the body, she said, such "an invasive search should require reasonable suspicion."

An interesting supporting brief filed in the Arnold case by the Association of Corporate Travel Executives and the Electronic Frontier Foundation said there had to be limits on the government's ability to acquire information.

"Under the government's reasoning," the brief said, "border authorities could systematically collect all of the information contained on every laptop computer, BlackBerry and other electronic device carried across our national borders by every traveler, American or foreign." That is, the brief said, "simply electronic surveillance after the fact."

The government went even further in the case of Sebastien Boucher, a Canadian who lives in New Hampshire. Boucher crossed the Canadian border by car about a year ago, and a customs agent noticed a laptop in the back seat.

Asked whether he had child pornography on his laptop, Boucher said he was not sure. He said he had

downloaded a lot of pornography but had deleted child pornography when he found it.

Some of the files on Boucher's computer were encrypted using a program called Pretty Good Privacy, and Boucher helped the agent look at them, apparently by entering an encryption code. The agent said he had seen lots of revolting pornography involving children.

The government seized the laptop. But when it tried to open the encrypted files again, it could not. A grand jury instructed Boucher to provide the password.

But a federal magistrate judge quashed that instruction in November, saying that requiring Boucher to provide it would violate his Fifth Amendment right against self-incrimination. Last week, the government appealed.

The magistrate judge, Jerome Niedermeier of U.S. District Court in Burlington, Vermont, used an analogy from Supreme Court precedent. It is one thing to require a defendant to surrender a key to a safe and another to make him disclose its combination.

The government can make you provide samples of your blood and handwriting and the sound of your voice. It can make you put on a shirt or stand in a lineup. But it cannot make you testify about facts or beliefs that may incriminate you, Niedermeier said.

Michael Fromkin, a law professor at the University of Miami, writing about the Boucher case on his Discourse.net blog, said, "The core value of the Fifth Amendment is that you can't be made to speak in ways that indicate your guilt."

But Orin Kerr, a law professor at the George Washington University, said Niedermeier had probably gotten it wrong.

"In a normal case," Kerr said in an interview, "there would be a privilege." But given what Boucher had already done at the border, he said, making him provide the password again would probably not violate the Fifth Amendment.

There are all sorts of lessons in these cases. One is that the border seems to be a privacy-free zone. A second is that encryption programs work. A third is that you should keep your password to yourself. And the most important is that you should leave your laptop at home.

Notes: