

Canadian Association of University Teachers
Association canadienne des professeures et professeurs d'université

CAUT Travel Advisory

U.S. Customs Searches of Electronic Devices at the Border and International Airports

September 2008

Tel 613/820-2270 Fax 613/820-7244 Email acppu@caut.ca



2705, promenade Queensview Drive
Ottawa (Ontario) K2B 8K2
www.caut.ca

U.S. Customs Searches of Electronic Devices at the Border and International Airports

Stories of U.S. Customs officials searching travelers' laptop computers at the Canada-U.S. border have been in the news lately and there have been conflicting U.S. court decisions about the legality of such searches under the U.S. Constitution. The issue is one of obvious concern for academics in Canada, who regularly travel to or through the United States for professional purposes, often carrying laptops and other kinds of electronic devices with them. While the U.S. Supreme Court has yet to rule directly on the matter, the 9th Circuit Court of Appeal has recently weighed in on the debate, bringing some clarity to the state of the law and suggesting the direction an eventual Supreme Court decision might take.

The *Arnold* Decision

In a decision released in April, 2008, the 9th Circuit Court of Appeal, reversing a lower court's judgment, held that the Fourth Amendment of the U.S. Constitution guaranteeing the right against unreasonable search and seizure does *not* require government agents to have *any* grounds for suspicion before searching electronic devices at the U.S. border. The case, *United States v. Arnold*,¹ involved the search of a traveler's laptop by U.S. Customs agents, but the Court's decision could apply equally to the search and seizure of other electronic devices such as cameras, Blackberries, cell phones, iPhones and MP3 players. The decision is alarming because these devices can contain vast amounts of information, often of an intensely personal or revealing nature, such as letters, research documents, health and financial records, diaries, photographs, downloaded songs and broadcasts, stored phone numbers and addresses, e-mails, web browsing records, customer records, proprietary information, information covered by solicitor-client or litigation privilege, and information about confidential sources or research subjects.

U.S. courts have long held that searches of persons and effects can be conducted at the border without probable grounds or even a reasonable suspicion of illegality. This body of law, known as the "border search doctrine" is an exception to the usual requirement under the Fourth Amendment that authorities have probable grounds and a judicial warrant before searching persons or property. A succinct statement by the U.S. Supreme Court of the doctrine and its history is contained in its judgment in *United States v. Flores-Montano*:

Time and again, we have stated that "searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border". Congress, since the beginning of our Government, "has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country".²

Searches of international passengers at American airports are considered border searches because they occur at the "functional equivalent of a border".³

Lawyers for Arnold argued that the search of a laptop computer is qualitatively different and more intrusive to personal privacy than the search of a suitcase or other physical item. Attempting to persuade the 9th Circuit Court of Appeal to impose some standard of suspicion to border searches of laptops, they asked it to draw distinctions between routine and non routine searches, invasive and less invasive searches, and searches of expressive and non expressive material. The Court rejected these arguments, relying on earlier Supreme Court decisions to do so.

First, the Court of Appeal noted that the Supreme Court in *Flores-Montano* had explicitly “rejected creating a balancing test based on a ‘routine’ and ‘non routine’ search framework”, and had clarified that its use of these terms in earlier cases had been intended as purely descriptive.⁴

Second, the Court of Appeal acknowledged that the Supreme Court had set limits on the border search doctrine in respect of searches of travelers’ alimentary canals. In *United States v. Montoya de Hernandez*, the Supreme Court held that reasonable suspicion is required to make such a search, because “[t]he interests in human dignity and privacy which the Fourth Amendments protects forbid any such intrusion [beyond the surface of the body] on the mere chance that desired evidence might be obtained”.⁵ However, the 9th Circuit Court of Appeal asserted that, in *Flores-Montano*, the Supreme Court had rejected the use of an intrusiveness analysis for *property* searches, stating that the “dignity and privacy interests” which supported “a requirement of some level of suspicion in the case of highly intrusive searches of the person” did not “carry over to [searches of] vehicles”.⁶ This had led the 9th Circuit Court of Appeal to go on to reject its own prior use of an intrusiveness analysis to determine the reasonableness of property searches in two subsequent vehicle search cases.⁷

Third, the Court of Appeal refused to carve out an exception to the border search doctrine for expressive material based on the First Amendment’s guarantee of freedom of speech. Citing the 4th Circuit Court of Appeal’s decision in *United States v. Ickes*⁸ (holding that no standard of suspicion is required for the search of expressive material contained in a laptop computer at the border), the 9th Circuit Court of Appeal concurred with its sister court’s reasoning that a First Amendment exception to the border search doctrine would:

- 1) protect terrorist communications which are inherently expressive;
- 2) create an unworkable standard for government agents who would have to decide – on their feet – which expressive material is covered by the First Amendment; and
- 3) contravene the weight of Supreme Court precedent refusing to subject government action to greater scrutiny with respect to the Fourth Amendment when an alleged First Amendment interest is also at stake.⁹

According to the 9th Circuit Court of Appeal the only two grounds left open by the Supreme Court to argue that a suspicionless search of property at the border is unreasonable are that the search was particularly destructive or that it was conducted in a particularly offensive manner.

¹⁰ In this regard, the Court held that there was no damage done in the search of Arnold’s laptop and that “case law does not support a finding that a search which occurs in an otherwise ordinary manner, is ‘particularly offensive’ simply due to the storage capacity of the object being searched”.¹¹

What the U.S. Supreme Court Might Rule

In summary, there now exist two court of appeal decisions, *Ickes* and *Arnold*, which hold that suspicionless searches of laptops at the border do not violate the Fourth Amendment guarantee against unreasonable search and seizure, as well as a handful of supporting court of appeal cases and the Supreme Court's *dicta* in *Flores-Montano*, which suggest that a sliding scale test of intrusiveness cannot be applied to searches of property, as opposed to searches of the person.

These cases are not the final word, however, because the Supreme Court has yet to rule on the exact issue (searches of laptops and other electronic devices at the border) and, in the meantime, the issue could come before other courts of appeal which might find a creative path through the precedents and decide the issue differently than *Ickes* and *Arnold*. For example, other courts of appeal could find that the Supreme Court's judgment in *Flores-Montano* is limited in application to vehicles and go on to distinguish electronic devices from vehicles and other kinds of property on the basis that the scope and nature of the material they contain *do* engage dignity and privacy interests and so should be subject to a sliding intrusiveness analysis. In a similar vein, other courts of appeal might accept that the content of electronic devices is similar in scope and nature to the content of a home or the human mind, so that suspicionless searches of these devices are inherently offensive. Alternatively, other courts of appeal might uphold a First Amendment exception to the border search doctrine because of the extent to which suspicionless searches of electronic devices chill freedom of expression.

If the issue does come before the Supreme Court, it could revisit and even overturn its earlier decisions. But, this is unlikely given the historic resistance of the Court to create exceptions to the border search doctrine.¹² Moreover, the Court will be keen to stop child pornography at the border and, especially, to prevent future terrorist attacks on American soil. In *Flores-Montano*, the Supreme Court observed that "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border".¹³ So, too, is American concern for homeland security at the present time.¹⁴

How Concerned Should Travelers Be?

Travelers may take some comfort in the 4th Circuit Court of Appeal's observation that "[c]ustoms agents have neither the time nor the resources to search the contents of every computer."

¹⁵ However, there is still cause for concern. One percent of executives surveyed recently by the Association of Corporate Travel Executives said their laptops had been confiscated at the international border¹⁶ and news stories of travelers having their laptops seized and returned days later, or not at all, are accumulating. Individuals fitting certain profiles may be particularly vulnerable to repeated searches at the border. For example, academics who travel regularly to certain countries or with origins in certain countries; academics with security or Middle East-related research interests; and those whose appearances suggest certain ethnic or religious backgrounds. U.S. Customs has stated publicly that it does not racially or ethnically profile travelers, but its officers' training guide states that "it is permissible and indeed advisable to consider an individual with connections to countries that are associated with significant terrorist activity."¹⁷

One can also be flagged for secondary inspection and the search of an electronic device through watch lists, risk scoring and data mining programs. The U.S. Terrorist Screening Center

reportedly manages 950,000 names on a consolidated watch list.¹⁸ The size of the U.S. No Fly list has crept up to an estimated 50,000 to 350,000 names,¹⁹ and the FBI's National Crime Information Center, the country's largest criminal justice database, reportedly contains over 39 million records.²⁰ The U.S. Automated Targeting System assigns risk scores out of a possible 100 points to all travelers at the international border based on undisclosed criteria and the U.S. Transportation Administration receives passenger name record information about air travelers which can contain up to 65 fields of information. A proliferating number of data mining programs run by U.S. agencies, using computer algorithms to sort through public and commercial information for specified relationships and patterns, could also flag one as a person of interest.

A final and substantial concern about searches of electronic devices at the border is that it is not yet clear under what authority and circumstances the U.S. government copies and stores data, shares it with other governments or might use it in the future. These questions are currently the subject of a Freedom of Information request filed by the Association of Corporate Travel Executives and a lawsuit initiated by the Electronic Frontier Foundation and the Asian Law Caucus.²¹ The Senate Judiciary Subcommittee on the Constitution, Civil Rights and Property Rights started hearings in June 2008 on the issue of "Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel", but there is little likelihood that Congress will introduce legislation which will protect non American travelers any time soon.

Limited Solutions

In the face of the concerns outlined above there are, unfortunately, only limited solutions. Of course, the safest option would be to leave one's laptop and other electronic devices at home if one is concerned about having them confiscated or their contents copied and scrutinized, and to either borrow or maintain back-up devices at one's destination. However, this is an unrealistic solution for many travelers and for academics, in particular.

Other options provide less protection, but are worth serious consideration. According to the *Washington Post*, "[a]t least two major global corporations, one American and one Dutch, have told their executives not to carry confidential business material on laptops on overseas trips ... In Canada, one law firm has instructed its lawyers to travel to the United States with 'blank laptops' whose hard drives contain no data".²² The lawyers access their information through the Internet, though this, of course, poses risks of hacking and interception. As well, experts suggest that even if one uses remote servers, traces, such as temporary files of Word documents, will remain on the laptop's hard drive and could be recoverable through forensic examination.²³

Some commentators have suggested using encryption, but refusal to provide Customs agents with an encryption key would be cause for denial of entry, just as refusal to hand over a user ID or password would.

In the end, the decision about what course of action to take must rest on one's assessment of the consequences which could ensue if Customs or security agents gained access to the contents of one's computer.

Endnotes

¹ 2008 WL 1776525

² 541 U.S. 149 (2004), citing *United States v. Ramsey*, 431 U.S. 606 at 616 (1977) and *United States v. Montoya de Hernandez*, 473 U.S. 531 at 537 (1985).

³ *Almeida-Sanchez v. United States*, 413 U.S. 266 at 273 (1973).

⁴ See *Flores-Montano*, *supra* note 2 at 152.

⁵ *Supra* note 2 at 540.

⁶ *Flores-Montano*, *supra* note 2 at 152.

⁷ *United States v. Chaudhry*, 424 F. 3d. 1051 at 1054 (2005) and *United States v. Cortez-Rocha*, 394 F. 3d. 1115 at 1122-1123 (2004, amended 2005). Petition for writ of certiorari denied, *Chaudhry v. United States*, 547 U.S. 1083 (2006); petition for writ of certiorari denied, *Cortez-Rocha v. United States*, 546 U.S. 849 (2005).

⁸ 393 F. 3d. 501 (2005).

⁹ *Ibid.* at 506-508, citing *New York v. P.J. Video*, 475 U.S. 868 (1986), in which the Supreme Court refused to require a standard higher than the usual probable cause standard for warrant applications involving expressive material.

¹⁰ Citing *Flores-Montano*, *supra* note 2 at 155-156 and *United States v. Ramsey*, 431 U.S. 606 at 618.

¹¹ Citing *California v. Acevedo*, 500 U.S. 565 at 576 (1991), in which the Supreme Court refused to find that "looking inside a closed container" when already properly searching a car was unreasonable.

¹² See *Flores-Montano*, *supra* note 2 upholding the doctrine of suspicionless searches where a car fuel tank was disassembled, removed and reassembled; *Carroll v. United States*, 267 U.S. 132 (1925), upholding the doctrine where the interior of a car was destroyed by Prohibition agents; and *Montoya de Hernandez*, *supra* note 2, in which the Court refused to decide what, "if any" suspicion might be requires for strip, body cavity and x-ray searches.

¹³ *Supra* note 2 at 152.

¹⁴ See, for example the extensive quotes about the case of Ahmed Ressam from the 9-11 Commission Report in *United States v. Cortez-Rocha*, *supra* note 7, a case which involved contraband whiskey, not terrorist activity.

¹⁵ *Ickes*, *supra* note 8.

¹⁶ Editorial, "Looking into Laptops", *Los Angeles Times*, (11 November 2006).

¹⁷ Ellen Nakashima, "Clarity Sought on Electronic Searches", *Washington Post*, (7 February 2008).

¹⁸ Evan Perez and David Crawford, "Europe Bristles at U.S. Security", *Wall Street Journal*, (9 June 2008).

¹⁹ BBC News, "US 'to halve' no-fly watch list", (18 January 2007), online: BBC News <<http://news.bbc.co.uk/2/hi/americas/6274221.stm>>.

²⁰ Bruce Schneier, "National Crime Information Center (NCIC) Database Accuracy", *Crypto-Gram*, April 15, 2003, online: <http://www.schneier.com/crypto-gram-0304.html>.

²¹ Nakashima, *supra* note 17.

²² Nakashima, *supra* note 17.

²³ Helen Burnett, "U.S. Border guards can look into your laptop", *Law Times*, (25 September 2006).