

Questions about E-Discovery?
E-DISCOVERY

For the answers, visit Law.com's FREE
ROAD MAP

LEGALTECHNOLOGY

Select 'Print' in your browser menu to print this document.

©2006 Law.com Legal Technology

Page printed from: <http://www.law.com/tech>

[Back to Article](#)

At the Border, Your Laptop Is Wide-Open

David E. Brodsky, Timothy M. Haggerty and Tamara J. Britt
The National Law Journal
July 22, 2008

After two of its executives had their laptops and other electronic devices seized and searched at U.S. airports in May, BAE Systems PLC -- the U.K.-based defense and aerospace giant -- found itself facing a travel risk that many companies had never considered: that U.S. officials could search, inspect and copy data from international travelers' electronic devices without a warning or warrant.

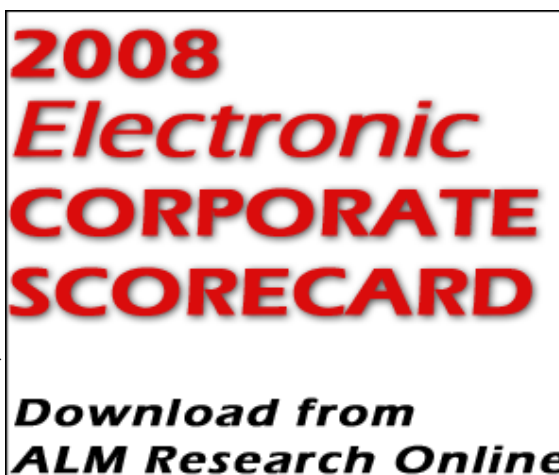
For BAE, the searches signaled an escalation in the Justice Department's high-profile, yearlong investigation into allegations of foreign corrupt payments. For the rest of the international business community, they signaled what may be a new trend in law enforcement. With increasingly global companies and increasingly portable technology, these searches would let the government access any data that travelers bring across the border on their laptops, BlackBerrys, cellphones or other electronic devices -- without warrants, probable cause or reasonable suspicion.

The searches raise legal questions that are making their way into Congress and the courts. In June, the Senate Judiciary Committee's subcommittee on the Constitution held a hearing on laptop searches at airports. Two months earlier, the 9th U.S. Circuit Court of Appeals joined the 4th Circuit in affirming the government's authority to conduct warrantless, suspicionless laptop searches at international airports. As the issue gains attention, companies are considering whether their travel and computing policies protect confidential corporate data against the risk that it will be searched and seized when employees enter the United States.

Although no court has considered whether an airport laptop search is constitutional when conducted in furtherance of an ongoing criminal investigation, several courts have reviewed warrantless, suspicionless laptop searches when conducted as part of routine customs inspections. Those courts have held that searches of laptops are no different than traditional warrantless searches of luggage or other property, meaning that they require no warrant, probable cause or reasonable suspicion when they are conducted at the border, or at an international airport, which courts consider the functional equivalent of the border. See *Almeida-Sanchez v. U.S.*, 413 U.S. 266, 273 (1973).

Laptop searching is a new development, but the government's plenary authority to conduct searches at the border is not. See *U.S. v. Ramsay*, 431 U.S. 606, 619 (1977) (border searches, "from before the adoption of the Fourth Amendment, have been considered to be 'reasonable' by the single fact that the person or item in question had entered into our country from outside"). That authority derives from the nation's "sovereign" and "inherent authority to protect, and [its] paramount interest in protecting, its territorial authority." See *U.S. v. Flores-Montano*, 541 U.S. 149, 153 (2004). The U.S. Supreme Court has held that routine searches at the border, whether of persons or property, are unlike most other searches of homes, persons, things or vehicles, and that they require no probable cause, reasonable suspicion or warrant. See *U.S. v. Montoya de Hernandez*, 478 U.S. 531, 538 (1985) (noting that the reasonable expectation of privacy is diminished at the border).

The court has suggested only two types of border searches that might be unconstitutional. In *Montoya de*



Hernandez, it held that some searches of the human body may be so intrusive that they implicate individual privacy and dignity interests, and therefore must be supported by reasonable suspicion. See *Montoya*, 478 U.S. at 538-40 (reviewing search of "alimentary canal"). The court has declined thus far to expand this exception to searches of property. See *Flores-Montano*, 541 U.S. at 152 (rejecting argument that reasonable suspicion was required for the removal, disassembly, inspection and reassembly of the gas tank of the defendant's vehicle). At least one circuit court has squarely held that the exception created in *Montoya de Hernandez* does not apply to property searches. See, e.g., *U.S. v. Chaudhry*, 424 F.3d 1051, 1054 (9th Cir. 2005).

The second type of border search that might require a threshold showing exists only in Supreme Court dicta. In several cases, the court has noted that a border search might become unreasonable "because of the particularly offensive manner [in which] it is carried out." See *Ramsay*, 431 U.S. at 618 n.13 (1977); *Flores-Montano*, 541 U.S. at 154-55 n.2.

BRIEFCASE ANALOGY

Against this backdrop, both circuit courts that have considered the constitutionality of border laptop searches have held that the searches do not require reasonable suspicion or probable cause. Rather, they have held that the searches are akin to the types of warrantless, suspicionless property searches the Supreme Court has expressly authorized, such as searches of travelers' suitcases, briefcases, pockets, papers and films. See *U.S. v. Arnold*, 523 F.3d 941 (9th Cir. 2008), petition for reh'g en banc filed, No. 06-50581 (9th Cir. June 2, 2008); *U.S. v. Ickes*, 393 F.3d 501 (4th Cir. 2005).

In so holding, these courts have rejected defendants' contentions that laptop searches are different, whether because of the massive amount of data they hold, the First Amendment implications of searching "expressive material" or the purported "invasiveness" of the searches. The court in *Arnold* found no reason that the amount of storage capacity would make an otherwise routine search "particularly offensive," and rejected the analogy between a laptop and a home as contrary to precedent and logic, noting dryly that "one cannot live in a laptop." See *Arnold*, 523 F.3d at 945 (citing *California v. Carney*, 471 U.S. 386, 393-94 (1984) [refusing to treat a mobile home as a "home" for Fourth Amendment purposes]).

As for the First Amendment arguments, the court in *Ickes* noted that an exception to the border-search doctrine based on "expressiveness" would "create a sanctuary at the border for all expressive material -- even for terrorist plans" and it would be practically unworkable because it would require border officials to make near-instantaneous determinations between materials protected by the First Amendment and those that are not. See *Ickes*, 393 F.3d at 506.

These courts have reasoned that a contrary result would create a rule by which a document's degree of protection is determined by the physical form that it takes -- a document on a USB thumb drive would be more closely protected than the same document printed on paper. The holdings of *Arnold* and *Ickes* are consistent with those of every district court to consider the issue. In some cases, courts have found that they need not resolve whether border laptop searches require reasonable suspicion because the government actually possessed reasonable suspicion for the challenged searches. See, e.g., *U.S. v. Irving*, 434 F.3d 401 (2d Cir. 2005); *U.S. v. Bunty*, No. 07-641, 2008 WL 2371211, at *3 (E.D. Pa. June 10, 2008); *U.S. v. McAuley*, No. DR-07-CR-786(1), 2008 WL 2387979, at *4-*6 (W.D. Texas June 6, 2008).

Arnold, *Ickes* and all of the lower court decisions that have considered the constitutionality of warrantless, suspicionless border laptop searches have involved searches that revealed child pornography, meaning that the defendants had committed crimes simply by carrying their computers into the country. See 18 U.S.C. 2252(a)(1).

A different situation arguably is presented when, as in the BAE case, the government searches a traveler's computer and copies its contents as part of an ongoing criminal investigation. In such a situation, the search does not relate to the nation's sovereign interest in protecting its borders against the importation of contraband (such as child pornography) or dangerous items (such as terrorist materials). Instead, the search serves a distinctly different government interest -- in securing evidence in an ongoing criminal investigation of the traveler's corporate employer. That interest, and the criminal investigation itself, may have nothing to do with border or national security.

Moreover, these airport laptop searches permit law enforcement to inspect massive amounts of private information in a way that conventional investigative techniques -- such as search warrants and subpoenas -- do not. Search warrants must be based on probable cause and typically include procedures for minimizing the searching of nonpertinent and privileged data, while grand jury subpoenas must specify the material sought and, at least theoretically, can be challenged in court.

CHORUS OF COMPLAINT

Before the BAE episode highlighted the possibility that airport laptop searches could become a tool in government's law enforcement arsenal, searches of laptops during routine customs inspections had begun to prompt complaints. The *Washington Post* in February recounted several border searches that travelers found invasive and disruptive, including one instance in which the traveler's computer had not been returned more than one year after it was seized. Ellen Nakashima, "Clarity Sought on Electronics Searches," *Washington Post*, Feb. 7, 2008, at A1. Other articles and commentary in the press have focused on similar episodes and advised readers how to avoid them.

The issue has not gone unnoticed by Congress. During a hearing in June, the Senate Judiciary Committee's subcommittee on the Constitution examined the legal and practical implications of border laptop searches. The overall tenor of the hearing was reflected in its title: "Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel." While the legal analysts before the subcommittee opined that the Supreme Court would be unlikely to disagree with the circuit courts' holdings in *Arnold* and *Ickes*, Senator Russ Feingold, D-Wis., the subcommittee's chairman, suggested that the border-search exception to the warrant requirement needs limits.

"I guarantee you this: neither the drafters of the Fourth Amendment, nor the Supreme Court when it crafted the 'border search exception,' ever dreamed that tens of thousands of Americans would cross the border every day, carrying with them the equivalent of a full library of their most personal information. ... If you asked most Americans whether the government has the right to look through their luggage for contraband when they are returning from an overseas trip, they would tell you yes, the government has that right. But if you asked them whether the government has a right to open their laptops, read their documents and e-mails, look at their photographs, and examine the Web sites they have visited, all without any suspicion of wrongdoing, I think those same Americans would say that the government absolutely has no right to do that. ... Ideally, Fourth Amendment jurisprudence would evolve to protect Americans' privacy in this once unfathomable situation. But if the courts can't offer that protection, then that responsibility falls to Congress." See "Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel Before the Senate Comm. on the Judiciary Subcomm. on the Constitution," 110th Cong. (June 25, 2008) (hereinafter "hearing") (statement of Sen. Russ Feingold, chairman, Subcomm. on the Constitution).

Other testimony focused on the policy concerns raised by these searches and recommended legislative and administrative changes. Several witnesses proposed legislation requiring reasonable suspicion for any laptop search and probable cause for any data seizure. Hearing (statement of Peter P. Swire, senior fellow, Center for American Progress Action Fund and professor of law, Ohio State University Moritz College of Law); (statement of Susan K. Gurley, executive director, Association of Corporate Travel Executives); (statement of Lee Tien, senior staff attorney, Electronic Frontier Foundation).

Many witnesses criticized the lack of transparency in customs practices. Customs and Border Patrol Deputy Commissioner Jayson P. Ahern, however, submitted testimony stating that the border laptop searches have been successful: "In addition to several successes in arresting individuals possessing child pornography, CBP border searches also have been helpful in limiting the movement of terrorists, individuals who support their activities and threats to national security. During border searches of laptops, CBP officers have found violent jihadist material, information about cyanide and nuclear material, video clips of Improvised Explosive Devices (IEDs) being exploded, pictures of various high-level al-Qaida officials and other material associated with people seeking to do harm to U.S. and its citizens." See Hearing (statement of Jayson P. Ahern, deputy commissioner, Customs and Border Patrol).

He added that customs has neither the need nor the resources to search every laptop at the border, so the searches that are conducted are "often premised on facts, circumstances and inferences which give rise to individualized suspicion, even though the courts have repeatedly confirmed that such individualized suspicion is not required under the law."

Feingold remarked that Ahern's testimony "provide[d] little meaningful detail on the agency's policies." Such information has been sought before. In February, the Electronic Frontier Foundation and the Asian Law Caucus sued the Department of Homeland Security for denying access to the department's records concerning its policies on the questioning, search and inspection of travelers entering the United States. See *Asian Law Caucus v. U.S. Dep't Homeland Sec.*, No. 08-CV-0842 (N.D.N.Y. filed Feb. 7, 2008). Other groups have said that the only information they have about DHS policies and procedures is anecdotal.

Apart from the publication of these policies, the witnesses recommended various limits on the duration and location of searches (i.e. away from public view), the qualifications of the searchers and the rules in place to prevent damage to the devices being searched. The witnesses also advised Congress to consider how travelers are being selected for these searches. In particular, Farhana Y. Khera, president and executive director of Muslim Advocates, described complaints that the organization has received about discriminatory application of electronic searches and seizures at border crossings. See Hearing (statement of Farhana Y. Khera, president and executive director, Muslim Advocates). The recommendations applied to any data copied by the authorities. Specifically, they included limits on the length of time any copied data would be stored and in defining the circumstances in which the data would be shared with other agencies.

Since the hearing, commentators have intensified the focus on the legal and policy issues the searches raise. The *New York Times* called the *Arnold* decision "disappointing" and opined that "[t]hese out-of-control searches trample the privacy rights of Americans, and Congress should rein them in." Editorial, "The Government and Your Laptop," *New York Times*, July 10, 2008, at A20. The government's ability to conduct searches depends on its ability to know where and when targeted individuals will arrive in the United States. This information was made more readily available as a result of the interagency information sharing implemented following the 2001 terrorist attacks. The traveler data that airlines report to the DHS is available to other federal agencies, and these agencies can use the information to track and meet targeted individuals when they enter the country.

The issue is not unique to the U.S. border crossings. Routine, suspicionless border searches of electronic equipment have been reported in China, England, Canada and Australia. See Chris Nutall, "UK Customs Check for Laptop Porn," BBC News Online Network, Aug. 13, 1998; Editorial, "Snooping in iPods," *Winnipeg Free Press*, May 29, 2007, at A12; "UK Engineer on Child-Porn Charges," *Daily Mail* (U.K.), Aug. 3, 2007, at 44.

LEAVE THE LAPTOP AT HOME?

This prospect of laptop searches at border crossings in the United States and elsewhere has prompted companies to review their travel and computing policies. Some companies have adopted policies intended to limit the data that the government could discover at a border search. The *Washington Post* reported that at least two companies have instructed executives to keep confidential business information off their traveling laptops. Nakashima, *supra*. An industry group has reported increased use of computers that can be "scrubbed" before travel. Companies may shift to Internet-based solutions whereby programs, files and e-mail are hosted on a central network instead of on the user's local hard drive.

All of these work-arounds pose a risk that residual files will exist on the user's computer and remain recoverable

through forensic searching. Other suggestions, such as stronger encryption of files, are not without risks. If a traveler refuses to turn over his or her passwords or encryption key, customs officials could detain the traveler, seize the laptop or, in the case of a foreign traveler, refuse entry to the country altogether. In light of these challenges, some companies are advising executives to follow the safest course of all -- leave the laptop at home.

It remains to be seen whether the type of targeted, investigation-specific laptop search used in the BAE case was an aberration or the start of a law enforcement trend. International companies would be well-advised to monitor this issue and consider evaluating whether their travel and computing policies adequately protect the sensitive and confidential information that their employees carry across the border on their laptops, BlackBerrys and other mobile electronic devices.

David E. Brodsky is a partner, Timothy M. Haggerty is an associate and Tamara J. Britt is a summer associate at New York-based Cleary Gottlieb Steen & Hamilton.

Subscribe to The National Law Journal