Bloomberg BNA

Criminal Law Reporter™

SEARCH AND SEIZURE

Border Insecurity: Searches and Seizures of Electronic Devices Entering the U.S.

BY LEE G. DUNST AND RACHEL BROOK

Travelers to the U.S. traditionally have been subject to the possibility of searches at the border when entering the country, but several recent court decisions have addressed the specific question regarding the limited legal protections afforded during government examination of the contents of laptops, mobile phones and other electronic devices in the possession of international travelers. Some of these recent decisions are in conflict, but they reinforce the general principle that electronic devices in the possession of people entering the U.S. may be subject to broad review by government authorities with limited protections under the U.S. Constitution and applicable laws and regulations.

Lee Dunst is a partner in the New York office of Gibson, Dunn & Crutcher, LLP. Dunst is a member of the firm's Litigation Department and White Collar Defense and Investigations Practice Group and previously served as an assistant U.S. attorney in the Eastern District of New York. Rachel Brook is an associate in the New York office of Gibson, Dunn & Crutcher, LLP and practices in the firm's Litigation Department and White Collar Defense and Investigations Practice Group. Contact ldunst@gibsondunn.com or rbrook@gibsondunn.com.

According to analysis of the most recent U.S. government statistics, the electronic devices in the possession of more than 6,500 people entering this country were searched by government officials during an 18-month period from October 2008 through June 2010.[1] For the most part, these investigative techniques appropriately target serious criminal offenses, such as terrorism and child pornography. But in light of the many international white collar criminal investigations now being conducted by the Department of Justice and the Securities and Exchange Commission, this broad power to capture electronic data at the border poses a particular risk for business executives and lawyers traveling into the U.S. This article reviews the current state of the law in this area, including a notable decision issued recently in federal court in Brooklyn, N.Y., *Abidor v. Napolitano*, No. 1:10-cv-04059-ERK, Dkt. 36 (E.D.N.Y. Dec. 31, 2013), and offers practical advice for practitioners and corporate executives traveling into the U.S. to limit the possibility that electronic data in their possession is exposed to U.S. government regulators.

The Standard: Little or No Suspicion Required

The Fourth Amendment to the U.S. Constitution provides, ''The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.'' To determine whether a search or seizure is unreasonable, courts balance the privacy interests of individuals against the governmental interests involved. Courts consistently have recognized that the government's interest is at its peak at the international border where the prevention of entry of unwanted people and material into the country is the primary goal. And courts have noted that there is also a significant public interest in effective preventive measures at the border. Conse-

[1] See ACLU, Government Data About Searches of International Travelers' Laptops and Personal Electronic Devices (Aug. 25, 2010), at https://www.aclu.org/national-security/government-data-about-searches-international-travelers-laptops-and-personal-electr.

 ISSN 0011-1341

quently, at the U.S. border, the Fourth Amendment's reasonableness balance tips in favor of the government's interest, and routine searches of people and items in their possession are permissible even in the absence of reasonable suspicion, probable cause, or a warrant—which the courts have referred to as the ''border search doctrine.''

On the other hand, courts have recognized that Fourth Amendment protections are of great importance ''where . . . the property to be searched is a computer hard drive.'' *United States v. Galpin*, 720 F.3d 436, 446 (2d. Cir. 2013). In fact, ''advances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain,'' the *Galpin* court said. As a result, courts recognize that ''the potential for privacy violations occasioned by an unbridled, exploratory search of a hard drive is enormous,'' the court said in *Galpin*. But courts continue to find that the governmental interest in national protection outweighs this privacy interest, and regulations allow for the possibility of suspicionless searches of electronics at international borders.

In August 2009, both U.S. Immigration and Customs Enforcement and U.S. Customs and Border Protection issued directives explicitly authorizing the search and seizure of electronic devices at international borders ''with or without individualized suspicion.'' ICE Directive No. 7-6.1, § 6.1; CBP Directive No. 3340-049, § 5.1.2. These directives allow for ''the inspection of any files and images stored on electronic devices, the performance of searches on the electronic devices, the detainment of electronic devices for a reasonable time to perform such searches, and the copying of stored information to facilitate inspection,'' the court recently said in *Abidor*.

Prior to these recent CBP and ICE regulations, Judge Lewis A. Kaplan of the U.S. District Court for the Southern District of New York held that laptop computers are equivalent to other closed containers subject to routine border searches without reasonable suspicion or probable cause. *United States v. Irving*, No. S3-03-0633, 2003 WL 22127913, at *5 (S.D.N.Y. Sept. 15, 2003). The *Abidor* court also recognized that ''laptop searches have proven essential to detecting people and materials that should be blocked from entering the United States,'' such as video clips reflecting terrorist activities and child pornography, both of which have been found through routine border searches of electronic devices.[2]

The U.S. Court of Appeals for the Second Circuit later affirmed Kaplan's *Irving* decision, finding, in particular, that searches of two computer discs were permissible. *United States v. Irving*, 452 F.3d 110, 124 (2d Cir. 2006). However, in *Irving*, the Second Circuit did not opine on the appropriateness of border searches of electronics without reasonable suspicion because it found reasonable suspicion existed in that case. Three other circuit courts have addressed this issue head on. The Third and Fourth Circuits have both held that electronic devices may be searched without reasonable suspicion as part of a routine border search. *United States v. Linarez-Delgado*, 259 F. App'x 506 (3d Cir. 2007); *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005).

The Ninth Circuit is the outlier, recently holding that reasonable suspicion may be required for border searches of electronic devices in certain circumstances. *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) (en banc). The Ninth Circuit distinguished between ''quick look'' searches of electronics versus ''forensic examinations,'' which are more extensive, exhaustive searches of a copied hard drive that intrude on privacy to a greater degree. The court held that ''forensic examination'' searches require reasonable suspicion, which was present based on the facts in that case.

The *Abidor* Decision

In *Abidor*, Judge Edward R. Korman of the U.S. District Court for the Eastern District of New York agreed that reasonable suspicion should exist before border patrol officers conduct more extensive searches of electronic devices. But he declined to make reasonable suspicion such a formal requirement for such searches at the border because, in practice, ''extremely limited resources available to conduct comprehensive forensic searches necessarily limits such searches to situations where some level of suspicion is present,'' Judge Korman said. This case is notable for many reasons, including its potential application to the tens of millions of people traveling annually through John F. Kennedy International Airport, which is located in the Eastern District of New York.[3]

The *Abidor* case involved a graduate student who, in May 2010, was traveling on an Amtrak train from Montreal to New York City when the train stopped at a CBP inspection point. After reviewing the student's customs paperwork and passport and asking several questions, a CBP officer requested that the student turn over his belongings, including a laptop, a digital camera, a hard drive and two mobile phones, for further inspection. All of the electronic items were searched during the five hours that the student was stopped at the checkpoint, and the laptop and hard drive were retained for 11 days for additional inspection and then mailed back to the student.

The inspection of the student's electronic devices was authorized by the 2009 CBP and ICE regulations that allow border patrol officers to conduct suspicionless searches of any electronic devices that travelers seek to carry across an international border. The student, along with two associations, one representing defense lawyers and the other representing photojournalists, brought a lawsuit seeking a declaratory judgment that the CBP and ICE policies violate the First and Fourth Amendments.

On Dec. 31, Judge Korman dismissed the case, holding that the CBP and ICE policies were constitutional and reasonable suspicion is not required for a cursory manual search of an electronic device at the border. Judge Korman emphasized that ''the Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border.''

Looking at the facts of the *Abidor* case, reasonable suspicion existed prior to the search of the student's electronic devices. In response to routine questioning, the student revealed that he had briefly lived in Jordan

[2] *Abidor*, at 27 (citing Michael Chertoff, *Searches Are Legal, Essential*, USA TODAY, July 16, 2008, at A10).

[3] See John F. Kennedy International Airport: Facts and Information, Statistics, available at http:www.panynj.gov/airports/jfk-facts-info.html (data from 2012).

  CRL ISSN 0011-1341

and visited Lebanon in the past year, but the U.S. passport that he presented to the CBP officer did not contain visas to these countries. Only after being questioned further about his travel did the student reveal that he also had a French passport in his possession, which held his visas for Jordan and Lebanon. At this point, the CBP officer asked the student to bring his belongings to a nearby location and conducted a ''quick look'' search of the electronic devices. During the inspection, the officer found photographs depicting rallies of Hamas and Hezbollah, both of which are designated by the State Department as terrorist organizations. The student explained that he had these images on his computer because he was researching the modern history of Shiites in Lebanon for his Ph.D. Consequently, the CBP officer retained the student's laptop and hard drive for further inspection by ICE, and the devices were returned to him 11 days later.

Judge Korman decided that there is currently no need for a formal reasonable suspicion requirement for border searches of electronics, given that most searches at the border are conducted de facto with reasonable suspicion such as that found in *Abidor*. But he said that in the event that ''suspicionless forensic computer searches at the border threaten to become the norm, then some threshold showing of reasonable suspicion should be required.'' In the meantime, the rule regarding border searches remains the same in most jurisdictions in the U.S.: Searches of electronic devices without suspicion are permissible.

Concerns: Individual Privacy Interests

The 2009 CBP and ICE regulations authorizing suspicionless searches of electronics at international borders have led to increased concern about the privacy of electronically stored personal information. Through such searches, authorities can obtain access to travelers' email accounts, bank accounts, Social Security numbers, personal photographs, passwords and work materials.

Special concerns have arisen for attorneys who travel for work, given their obligation to maintain the confidentiality of their clients' case files and information. The National Association of Criminal Defense Lawyers was one of the plaintiffs in *Abidor*. NACDL members are criminal defense attorneys who routinely travel internationally for professional purposes, carrying electronic devices that contain privileged and confidential client materials. In *Abidor*, NACDL argued that the CBP and ICE regulations interfere with its members' ability to represent their clients because they must consider the risk that client materials could be reviewed, copied and retained at the border by the government, which is often an adversary in cases or investigations.

Protecting Sensitive Electronic Information

While individual privacy concerns are compelling, U.S. courts find that the scale tips in favor of the governmental interest in monitoring the international borders, as do courts in many other countries around the world that also permit suspicionless border searches of electronics. For example, the United Kingdom Terror Law Schedule 7, § 8 authorizes searches of electronic devices without reasonable suspicion. Thus, even if laws in the U.S. required reasonable suspicion for border searches of electronics, people traveling internationally with devices would still risk searches at other international borders.

Moreover, another privacy risk to electronic data confronted by people, whether traveling abroad or not, is the risk of losing laptops and other devices. A study reported that more than 16,000 laptops are lost or mislaid in airports weekly by U.S., European and United Arab Emirates business travelers.[4] Thus, given the risk of loss or border search of a device, people should take steps to protect their electronically stored business and personal information. The 2009 ICE and CBP directives provide several protective measures for sensitive information, and there are other precautions that people can take on their own to safeguard their private data.

Protective Measures Provided by CBP and ICE Directives

The CBP and ICE directives provide guidelines for border searches of electronic devices aimed at minimizing intrusions of privacy. Both directives require that searches be completed within a reasonable time, which under the CBP rule is within five days and under the ICE rule is within 30 days. CBP Directive § 5.3.1; ICE Directive § 8.3(1). Before detaining or copying a device to continue a border search after a traveler leaves the border search site, the CBP officer must obtain supervisory approval, though such pre-approval is not required under the ICE directive. CBP Directive § 5.3.1.1.

Reasonable suspicion of a violation of laws enforced by the CBP or ICE must exist if a border patrol officer wants to share a device or information therein with another federal agency for assistance with determining the meaning or value of the information. CBP Directive § 5.3.2.3; ICE Directive § 8.4(2)(b). Additionally, the CBP directive requires supervisory approval prior to seeking such assistance. CBP Directive §§ 5.3.2.4.

The CBP and ICE directives both require that once information is reviewed, if it is found to be irrelevant (or in the case of CBP rules, it is found that no probable cause exists to believe the information is evidence or the fruit of a crime that CBP is authorized to enforce), all copies must be destroyed within seven days (seven business days for ICE) of the determination, unless special circumstances exist.[5] CBP Directive § 5.3.1.2; ICE Directive § 8.5(1)(e). Even where special circumstances exist, border patrol officers must obtain supervisory permission to hold the device or copies of information for more time, and copies still must be destroyed no later than 21 days after the determination. CBP Directive § 5.3.1.2; ICE Directive § 8.5(1)(e).

Finally, the CBP and ICE directives contain special provisions addressing the handling of privileged or sensitive materials, including legal materials, medical records and work-related information carried by journal-

[4] *Airport Insecurity: The Case of the Lost & Missing Laptops*, Ponemon Institute LLC, 3 (July 29, 2008), http://www.dell.com/downloads/global/services/dell_lost_laptop_study_emea.pdf.

[5] The CBP directive allows two categories of information to be retained without probable cause: (1) information regarding immigration, customs and other related enforcement matters; and (2) terrorism information, which can be provided to the federal agency responsible for analyzing such information. CBP Directive §§ 5.4.1.2 & 5.4.1.4.

ists. CBP Directive § 5.2; ICE Directive § 8.6. In the event that a border patrol officer encounters information on a device that appears to be legal in nature and possibly evidence of a crime or otherwise within CBP or ICE jurisdiction, CBP and ICE rules require the officer to seek advice from CBP or ICE counsel before conducting the search, and counsel will coordinate with the local U.S. Attorney's Office when necessary. CBP Directive § 5.2.1; ICE Directive § 8.6(2)(b). When encountering other potentially sensitive material, such as medical records or journalist work-related information, officers are required to abide by any applicable federal laws, and if they have any questions about how to handle the information, they must consult with CBP or ICE counsel. CBP Directive § 5.2.2; ICE Directive § 8.6(2)(c). And any business or commercial information found during searches of devices must be treated as business confidential and protected from unauthorized disclosure. CBP Directive § 5.2.3; ICE Directive § 8.6(2)(a).

Additional Measures Individuals Can Take

The only guaranteed way to protect personal and sensitive electronic data when traveling is to keep it at home. To state the obvious, that is not always possible. Privacy experts recommend that, when possible, travelers should remove any data from their electronic devices that they do not need prior to traveling. It is recommended that travelers first back up the information onto an external hard drive or other device. Subsequently, any materials not needed for the upcoming trip should be erased using a secure file erasure program to ensure that the removed items do not remain on the computer in temporary files or other hard-to-find locations. Additionally, web browsers can record the searches conducted by a user in cookies, caches and browser histories, and so these items should be cleared of recorded information prior to travel as well. Companies also can send employees on business trips with forensically clean laptops to limit the amount of proprietary information at risk.

However, ''clean'' electronic devices are often not a realistic option, particularly when traveling for business purposes, which requires the use of materials prepared and stored on laptops and other devices. To facilitate use of business documents while traveling, companies and individuals can use cloud storage (such as DropBox and CloudSafe) to store and work on sensitive business-related documents. They also can use virtual private networks (so-called VPNs) and shared drives, which provide access to private office networks over the Internet. These tools allow for use of documents without storage of those documents on the electronic devices carried during travel. Even if travelers choose to keep the majority of their materials on their devices, cloud storage, VPNs and shared drives can be utilized for the most sensitive information. Other options for protecting sensitive data on devices include setting up passwords, data encryption and partitioning of hard drives.

* * * *

As recent U.S. court decisions make clear, there are few protections for searches of the electronic devices that travelers bring into this country. While such broad investigative measures certainly are warranted for offenses involving terrorism or child pornography, this broad search power by the U.S. government creates serious privacy concerns for business executives and attorneys traveling into the U.S., which should be considered and addressed in advance (if possible), especially if the business at issue may be the subject of a white collar criminal investigation by U.S. regulators.

  CRL ISSN 0011-1341