THE GOVERNMENT CONTRACTOR®

THOMSON REUTERS

Information and Analysis on Legal Aspects of Procurement

Vol. 59, No. 27 **July 26, 2017**

Focus

¶ 223

FEATURE COMMENT: Electronic Device Searches: What Business Travelers Should Know About Searches And Seizures Of Electronic Devices At U.S. Borders And Airports

In the first six months of fiscal year 2017, U.S. border agents conducted 14,993 searches of electronic devices at borders and airports. This number is triple the total number of searches of electronic devices conducted in 2015.

With the frequency of electronic searches on the rise, it is important for companies to consider what information may be housed on the phones, tablets and computers carried by their employees or contractors traveling to or from the U.S., and to prepare for the possibility that these electronic devices may be searched and seized. We examine below some interactions that could happen when business travelers arrive or depart from U.S. borders and airports, and provide some practical tips on how to handle a border search and for safeguarding important data.

Of course, travelers will also need to understand the risks presented by entering other countries and take appropriate measures to protect electronic information. There may be further risk in that once information is in the hands of another country, that country may do little to protect it and could share it with other countries or private entities. A traveler may have little recourse for the return of information.

Arriving in the U.S.—*CBP*: Chief among the agencies responsible for manning U.S. borders and airports is U.S. Customs and Border Protection. CBP has the broad mission to "prevent terrorists and terrorist weapons from entering the country, provide security at U.S. borders and ports of entry, apprehend illegal immigrants, stem the flow of illegal drugs, and protect American agricultural and economic interests from harmful pests and diseases."

Commensurate with its mission of interdicting crime at the nation's borders, CBP enjoys broad authority to inspect travelers and their belongings. See 19 CFR § 162.6. CBP requires all travelers arriving at a "port of entry" to undergo "primary inspection"—a CBP officer checks a traveler's documentation and determines the traveler's admissibility to the country.

For the vast majority of travelers, interaction with CBP ends here. Some, however, are pulled aside for "secondary inspection"—that is, further questioning or a more intrusive look into their belongings. This may be because of a random screening or incomplete entry documents, or perhaps the CBP officer noticed something out of the ordinary. Whatever the reason, CBP does not have to disclose it to a traveler designated for secondary inspection.

It is during secondary inspection that CBP may attempt to search or seize a traveler's electronic devices. This may include requesting access to a specific file or information (such as an individual's list of contacts), requesting a password, reviewing the information contained in or linked to the device, or making a copy of the hard drive. CBP policy states that CBP "may detain electronic devices, or copies of information contained therein, for a brief, reasonable period of time to perform a thorough border search[, which] ordinarily should not exceed five (5) days."

Of course, most companies worry about their confidential information. Unlike luggage or a briefcase, a laptop or even a cell phone could contain information that is effectively the company's crown jewels. This is especially true if a device can be linked to cloud storage or mapped such that CBP can recover deleted items.

The courts have struggled with balancing travelers' privacy interest with the nation's border protec-

tion interest. Some courts have held that electronic devices should be treated like luggage, such that searches of electronic devices fall within the so-called "border search exception" to the warrant requirement of the Fourth Amendment. Other courts have held that "routine" searches of electronic devices, such as turning on the device and accessing unencrypted files, fall within the exception, but more intrusive "forensic" searches, such as those that recover deleted files, require reasonable suspicion.

How CBP treats business travelers also may depend on whether they are U.S. citizens. Citizens of the U.S. enjoy the "absolute right to enter its borders." *Tuan Anh Nguyen v. I.N.S.*, 533 U.S. 53, 67 (2001). Thus, although they may be searched and temporarily detained, U.S. citizens cannot be denied entry. Non-citizens, however, do not enjoy this privilege, and they may be searched, detained and turned away at the border. Accordingly, if non-citizens refuse to cooperate with a search—by declining to provide passwords, for example—they risk being turned away at the border.

Privileged Information: CBP has imposed some limits if electronic devices contain information protected by the attorney-client privilege or work-product protection. CBP directive "Border Search of Electronic Devices Containing Information" provides that legal materials are not exempt from a border search, but a special procedure may apply. That is, if the CBP officer *suspects* that the materials *may* contain evidence of a crime or other matter within CBP's jurisdiction, then the officer must first consult with CBP associate or assistant chief counsel. The standard for triggering the continued pursuit of legal information is not very high, and CBP does not provide guidance for how counsel is to assess such a situation. The American Bar Association has petitioned the Department of Homeland Security to provide more direction to protect confidential legal information.

Other Confidential Information: CBP acknowledges that electronic devices may contain other sensitive information, such as medical records, information carried by journalists, and business or commercial information. CBP directs officers to handle such information "in accordance with federal law and CBP policy," and to address any questions to CBP associate or assistant chief counsel. For confidential business information specifically, officers are to protect the information from unauthorized disclosure. These directives provide little guidance for the line officer making determinations at a border entry point.

Other Agencies and TSA: Other law enforcement agencies, such as the Federal Bureau of Investigation, or local law enforcement officials may be present in airports or at borders, but typically they will not be part of the entry screening process. However, CBP can "deputize" such officials, allowing them to participate in border searches.

Moreover, although they are not authorized to conduct border searches by themselves, non-CBP law enforcement agents may ask CBP officers to conduct a border search. Courts have held that a non-CBP agency that lacks probable cause to search may request a customs official to perform a border search on their behalf. See *U.S. v. Schoor*, 597 F.2d 1303, 1306 (9th Cir. 1979).

The Transportation Security Administration is tasked with "protecting the United States' air, land, and rail transportation systems to ensure freedom of movement for people and commerce." TSA, unlike CBP, is not a law enforcement agency. As such, its authority to search and seize items is limited to "establishing whether the passenger [or the passenger's luggage] is carrying unlawfully a dangerous weapon, explosive, or other destructive substance." TSA "[s]creening may not be conducted to detect evidence of crimes unrelated to transportation security."

In 2015, then-secretary of Homeland Security Jeh Johnson "directed TSA to implement enhanced security measures in the coming days at certain overseas airports with direct flights to the United States." In response, TSA announced that "officers may ask that owners power up some devices, including cell phones."

But TSA, historically at least, has rejected any notion that it searches and seizes electronic devices. TSA has stated that it "does not and will not confiscate laptops or other electronic devices .... We will not ask for any password, access to any files or take the laptop from you for longer than it takes to determine if it contains a threat." TSA further clarified that accusations about "how TSA officers ... can search the files on your laptop and can also confiscate your computer and copy your hard drive ... [are] not true." And it added that TSA officers are limited to "visually inspect[ing] your laptop and perform[ing] an explosives trace detection test." In sum, there presently is no TSA policy on search and seizure of electronic devices.

Company Policies and Advice to Employees—Travelers flying within the U.S. should not have to worry about TSA searching or seizing their electronic devices (unless, of course, law enforce-

ment has some other justification, such as a search warrant, to conduct a search). TSA has advised that "[s]hould anyone at a TSA checkpoint attempt to confiscate your laptop or gain your passwords or other information, please ask to see a supervisor or screening manager immediately."

Companies concerned about disclosure of data through employees traveling internationally should take actions that make access to files "non-routine." This may include:

- encryption or password-protection of sensitive information, i.e., adding a layer of security for e-mail accounts or files, beyond the password required to unlock a device;
- requiring that employees travel with a clean device and access sensitive information remotely once at their destination; or
- copying all files before traveling in the event the device is detained.

As a practical matter, given finite resources, a CBP officer is unlikely to go through the hassle of attempting to search protected information in the absence of reasonable suspicion of criminal conduct or other factors. One of those factors could be the nationality of the traveler. DHS Secretary John Kelly said in testimony before Congress earlier this year that foreign travelers coming into the U.S. should have to provide their passwords to electronic devices. As a legal matter, CBP attempts to access encrypted or password-protected data may render a search "non-routine" or "forensic" in nature, such that reasonable suspicion is required to justify invasive and extensive techniques. Although there were 23,877 electronic media searches last year, they amounted to only 0.0061 percent of total arrivals into the country.

Companies may also consider instructing employees or agents how to respond if CBP officers demand a traveler's help to access an electronic device. A traveler may refuse, but this could lead to extended detention of both person and property, or denial of entry into the country for non-U.S. citizens. Companies should consider who is traveling with their information (e.g., U.S. citizens or foreign citizens), the risks of disclosure and the costs of refusal.

- As a general matter, employees should try to establish a cooperative posture with CBP, while understanding the limits of what they can disclose.
- If CBP demands access to a device, employees should notify CBP agents of any sensitive or confidential business information contained on the device, particularly if that information is protected by the attorney-client privilege or work product doctrine.
- Employees should also ask to contact company counsel, although such request may be refused.
- U.S. citizen business travelers may refuse to help access the device if necessary to protect company information, although they should not physically withhold the device from CBP. Refusal to provide access likely will result in prolonged detention, and may mean that CBP will eventually keep the device while letting the employee proceed into the country. This may afford company counsel an opportunity to intervene to petition for the return of the device or ensure the destruction of any information obtained from it.
- Non-U.S. citizens will need to consider whether the information contained on a device is worth the cost of refusing to provide assistance—that is, prolonged detention, confiscation of the device and, potentially, exclusion from entering the U.S.
- If a device is detained, the employee should ask to speak to a CBP supervisor (a CBP officer needs permission from a supervisor to detain an electronic device after a person's departure) and ask for a Customs' receipt (Form 6051D).

Conclusion—The search and seizure of electronic devices at borders and other ports of entry raise difficult practical and legal questions. For business travelers and companies, they pose not only a hassle, but an existential concern about the privacy and security of their proprietary information. While companies and travelers can take steps to reduce their exposure, the best practice to ensure absolute security when crossing international borders may simply be not to bring any device containing sensitive information.

✦

This Feature Comment was written for THE GOVERNMENT CONTRACTOR by* Evelina Norwinski *and* Marcus Asner, *Partners in Arnold & Porter Kaye Scholer's White Collar Defense practice group; and* Andy Wang, *an Associate in Arnold & Porter Kaye Scholer's Litigation Group.* Nora Ellingsen, *a third year law student at Harvard Law School, contributed to this article.

