iWitness

BORDER SEARCHES AND THE LIMITS OF ENCRYPTION IN PROTECTING PRIVILEGED INFORMATION

STEVEN G. STRANSKY

The author is senior counsel at Thompson Hine LLP, Cleveland.

Do you encrypt your electronic devices before traveling abroad to protect sensitive or privileged information? Some of the more scrupulous attorneys among us do; they proactively encrypt their electronic devices containing privileged information to avoid the risk of intrusive searches by border patrol officers. But does this prevent sensitive information on your device from being reviewed by the authorities? Not fully. Although the use of encryption is an important data security practice for all attorneys, it may not protect privileged information from the highly sophisticated decryption tools readily available to intelligence agencies. In fact, a closer review of the federal policy governing the inspection of electronic devices at the border reveals that the U.S. intelligence community is authorized to assist border screening efforts by providing decryption and other technical services.

In recent years, several commentators and organizations, including ABA, have warned attorneys traveling internationally that they could be subject to intrusive searches by law enforcement when arriving at international borders, which consequently could implicate any privileged information in their possession. Some have recommended that attorneys encrypt their personal devices during international travel to avoid exposing privileged information during border screening. For instance, in its Formal Opinion 2017-5, the New York City Bar stated that before crossing the U.S. border, attorneys are required "to take reasonable measures . . . to avoid disclosing confidential information in the event border agents seek to search the attorney's electronic device," which include "using encrypted software to attempt to restrict access to mobile devices." Similarly, the ABA has recommended to attorneys who are traveling internationally with privileged information on an electronic device to consider locking the device and encrypting the information stored on it prior to border screening. However, analysis of the federal government's border search policy demonstrates that encrypting electronic devices may not significantly protect the information contained in them from government access and review during border screening operations.

Border Searches and the Law

Congress has broadly delegated to the executive branch the power to screen people and property at U.S. borders, which is primarily exercised through U.S. Customs and Border Protection (CBP). For example, 19 U.S.C. § 482(a) authorizes CBP officers, under certain conditions, to "stop, search, and examine . . . any vehicle, beast, or person," and 19 U.S.C. § 1496 authorizes the CBP to examine "the baggage of any person arriving in the United States in order to ascertain what articles are contained therein. . . ." Similarly, 19 U.S.C. § 1461 provides that all merchandise and baggage brought to the United States from "any contiguous country" must be "inspected by a customs officer" and that the officer may require the owner of any bag, luggage, or container "to open" or "to furnish a key or other means for opening" it for inspection.

The U.S. Supreme Court has routinely upheld this broad delegation of power. In *United States v. Flores-Montano* (2004), the Court ruled that "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." Accordingly, the Court has found a border search exception to the Fourth Amendment, which authorizes federal officials to conduct routine stops and searches at the border without a warrant, reasonable suspicion, or probable cause. Although CBP border officers do not require any suspicion of wrongdoing to conduct most routine border searches, the courts have indicated that highly intrusive, nonroutine searches can be undertaken only after satisfying the "reasonable suspicion" standard.

However, the nature and scope of intrusion that would transform a border search from routine to nonroutine is undefined and has been addressed by the courts only on a case-by-case basis.

Homeland Security Policy on Searching Electronic Devices

In January 2018, the CBP issued Directive No. 3340-049, Border Search of Electronic Devices, which governs how CBP officers may search electronic devices as part of their border inspection and screening mission. More specifically, section 5.2 of the directive sets forth the procedures on how CBP officers may search information that is subject to the attorney-client privilege or related to the attorney work-product doctrine. In these circumstances, CBP officers "shall ensure the segregation of any privileged material from other information examined during a border search to ensure that any privileged material is handled appropriately while also ensuring that CBP accomplishes its critical border security mission."

If, however, a CBP officer does gather and inspect privileged information, under section 5.2.1.3 of the directive, the officer is to "destroy" the information after the search is completed, unless the materials relate to "an imminent threat to homeland security" or need to be retained for litigation purposes or to satisfy other legal requirements. Unfortunately, the directive does not define "imminent threat to homeland security," which may be problematic for certain types of privileged information. For example, although privileged information concerning the legal defense in a criminal or terrorism matter may not be included in this exception, one cannot reach this conclusion based on the text of the directive alone. Moreover, the directive is silent as to whether privileged information involving lawsuits *against* CBP or other federal

Illustration by Dave Klug

agencies would trigger the litigation purpose exception.

As noted above, some attorneys encrypt devices as a means to avoid law enforcement scrutiny at the border. Section 5.3.3 of the directive addresses this issue and provides that if CBP officers are "unable to complete an inspection of an electronic device because it is protected by a passcode or encryption, the [o]fficer may, in accordance with section 5.4 [of the directive], detain the device pending a determination as to its admissibility, exclusion, or other disposition." In turn, section 5.4.2.1 provides that in circumstances where CBP officers need assistance to access a device's contents (e.g., for encrypted or password-protected devices), they may "convey electronic devices or copies of information therein" to third parties to seek "technical assistance."

Intelligence Community Support

The term "technical assistance" is quite significant. In fact, although the phrase "intelligence community" is never mentioned in the directive, section 5.4.2.1 indirectly references the types of technical support that intelligence agencies are authorized to provide to CBP officers as they perform their border inspection mission.

As background, Executive Order 12333, United States Intelligence Activities, is the primary presidential directive regulating how intelligence agencies conduct their missions and operations. As could be expected, it authorizes the intelligence community to provide direct support to federal officials across the executive branch. In particular, section 2.6 of the executive order authorizes intelligence agencies to provide specialized equipment, technical knowledge, and assistance of expert personnel to *any* federal department or agency, which includes the CBP.

To undertake many of their underlying foreign intelligence and counterintelligence assignments, elements of the U.S. intelligence community have a range of technical expertise, knowledge, and resources in the area of encryption. For instance, the National Security Agency (NSA) is the federal government's leading agency in the field of decryption and has been described as the nation's cryptologic organization. In addition to its better-known activities related to signals intelligence, the NSA is also responsible for coordinating, directing, and implementing highly specialized and technical activities related to information security. In short, the NSA is responsible for making and breaking the most technically challenging forms of encryption.

The Defense Intelligence Agency also has a significant role in this area as it serves as the chief intelligence agency at the National Media Exploitation Center, or NMEC as it is commonly termed. The NMEC is a forum consisting of representatives from multiple intelligence agencies and is responsible for merging intelligence resources to decrypt, translate, and analyze documents and electronic devices that are in the federal government's possession. According to U.S. Intelligence Community Directive 302, Document and Media Exploitation, the NMEC is required to provide these types of media exploitation services to satisfy the needs of "homeland security" and "law enforcement" officials, among them CBP officers and other possible border screening officials.

Traveling with Privileged Information and Risk Analysis

As noted above, document and media encryption is frequently used to safeguard sensitive information because it ensures that such information can be read or understood only by authorized users. However, it seems likely that the NSA or NMEC, given each agency's resources and expertise, has the technical capabilities to defeat standard encryption techniques. Accordingly, if CBP officers are seeking to decrypt and access information as part of their border screening function, they likely have the authority and technical resources (through the intelligence community) to do so.

This is not meant to imply, however, that traveling with privileged information raises an insurmountable risk or that CBP officers directly target lawyers for enhanced screening. According to the CBP Office of Public Affairs, in fiscal year 2017, only about 0.007 percent of arriving international travelers screened and processed by CBP officers had their electronic devices searched. In fiscal year 2016, that number amounted to only 0.005 percent of arriving international travelers. Consequently, for attorneys who are traveling internationally with privileged information on an electronic device, there is a low probability that this information will be subject to inspection and compromise. In such circumstances, the measures set forth by the New York City Bar and ABA may be sufficient to protect privileged information from unauthorized disclosure. However, for those still harboring concerns about having to either disclose privileged information or provide the device on which it is stored directly to CBP officers during a border search, it is important to recognize the limitations of encryption. In these situations, the best technique to ensure that privileged information is not compromised during a border search is not to possess it—in any form—at the time you encounter the CBP for inspection. ■

The best technique to ensure that privileged information is not compromised during a border search is not to possess it.