AMERICAN IMMIGRATION LAWYERS ASSOCIATION

Practice Pointer

BORDER SEARCHES OF ELECTRONIC DEVICES: LEGAL AND ETHICAL IMPLICATIONS AND SOLUTIONS (UPDATED 3/24/18)

On January 5, 2018, U.S. Customs and Border Protection (CBP) released an update to its directive governing border searches and electronic Devices. As the first directive issued since 2009, CBP has sought to find a balance between national security needs and the protection of legal and constitutional rights. Deputy Executive Assistant Commissioner, Office of Field Operations, John Wagner stated:

> *In this digital age, border searches of electronic devices are essential to enforcing the law at the U.S. border and to protecting the American people.... CBP is committed to preserving the civil rights and civil liberties of those we encounter, including the small number of travelers whose devices are searched, which is why the updated Directive includes provisions above and beyond prevailing constitutional and legal requirements. CBP's authority for the border search of electronic devices is and will continue to be exercised judiciously, responsibly, and consistent with the public trust.*[1]

Changes Made by the New Directive

Border Searches of Electronic Devices

- The new directive continues the April 2017 policy prohibiting officials from intentionally accessing information stored remotely. Border searches of electronic devices include searches of information stored on a device, not in the cloud. To avoid accessing information stored remotely, the traveler will be allowed to disable connectivity. CBP can also disable network connectivity when dealing with issues of national security.

- The new policy distinguishes between "basic" and "advanced" searches. An "advanced" search is "any search in which an Officer connects external equipment … to an electronic device not merely to gain access to the device but to review, copy, and/or analyze its contents.[2] CBP must have reasonable suspicion of unlawful activity or show that there is a "national security concern" in order to conduct advanced searches.

Review and Handling of Privileged or Other Sensitive Material

- The new directive limits review of information protected under attorney-client privilege. CBP should request clarification, (ideally in writing) from the party asserting

[1] CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics (Jan. 5, 2018), *available at* https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and.
[2] CBP Directive No. 3340-049A: Border Search of Electronic Devices (Jan. 4, 2018).

the privilege, which specific files, file types, folders, or categories of information that may be privileged. Privileged information must then be segregated by a designated "Filter Team," comprised of legal and operational personnel to ensure information is handled appropriately.

Review and Handling of Passcode-Protected or Encrypted Information

- The new directive requires travelers to "present electronic devices and the information contained therein in a condition that allows inspection of the device and its contents." Officers may request the traveler's assistance in providing passwords or other means of access to allow inspection. If inspection cannot be completed because the device cannot be accessed, CBP may detain the device pending determination of admissibility.

Detention and Review in Continuation of Border Search of Information

- CBP may detain an electronic device or copies of information for a reasonable period of time required to perform the border search. Supervisory approval is required to continue the search after the traveler has left the port of entry.

- CBP may request technical assistance to access and search the electronic device. The new directive does not place limitations upon what is considered "technical assistance" or who/what may provide it. CBP may also request "subject matter assistance" from experts if there is a reasonable suspicion that laws enforced by CBP have been violated or if there are national security concerns.

Evolution of the New Directive

Then Acting Commissioner, Kevin McAleenan directed the review of the agency's electronic device policy. Prior to his appointment, McAleenan appeared before the Senate Committee on Finance.[3] In response to questioning, McAleenan indicated that:

- CBP understands that electronic devices contain personal information and have operated under a policy directive which ensures that only information residing on the device is searched. CBP Directive 3340-049, "*authorizes CBP officers to transmit electronic devices or copies of information contained therein to other federal agencies only when they have reasonable suspicion of activities in violation of the laws enforced by CBP*." CBP is required to update its standard operating procedures relating to searches of electronic devices at POEs at least every 3 years and the directive will be revised to reflect "evolving operational practices."

- CBP has the authority to search electronic devices of U.S. citizens at the request of other governmental agencies. 19 CFR §162.6 provides that "*[a]ll persons, baggage and*

[3] U.S. Senate Committee on Finance, Hearing to Consider the Nomination of Kevin K. McAleenan, to be CBP Commissioner (Oct. 24, 2017), Questions for the Record.

merchandise arriving in the Customs territory of the United States from places outside thereof are liable to inspection and search by a Customs officer."

- CBP doesn't have a tracking mechanism to account for electronic device searches at the border with the assistance of another federal agency. While the number of searches has increased, CBP examines less than one-hundredth of one percent of U.S. bound travelers. Recent change in CBP policy is due to current threat information based upon intelligence. "As the threat landscape changes, so does CBP."

- A muster marked "For Official Use Only" has not been made public because it speaks to "internal operational policy and protocol and contains law enforcement sensitive material." McAleenan goes on to provide:

    - *CBP has explained publicly that its borders searches extend to information that is physically resident on the device, and does not extend to information that is solely located on remote servers (known as solely "in the cloud"), which is the subject of that muster...*

    - *Border searches of electronic devices extend to searches of the information residing on the physical device when it is presented for inspection or during its detention by CBP for a border inspection. To ensure the data residing only in the cloud is not accessed, officers are instructed to ensure that network connectivity is disabled to limit access to remote system*

- If CBP is unable to determine whether an electronic device is admissible, the officer may detain the electronic device and provide a custody receipt to the traveler.

- In response to written questions, McAleenan stated that CBP compares a request for a PIN or password to a request to open a briefcase or purse. CBP does not believe it has to inform a traveler of his or her right to refuse to provide a password or PIN. CBP believes that an inspection of an electronic device transported by an international traveler does not require the consent of the traveler.[4]

- U.S. citizens will not be prevented entry because of a refusal to provide a password to unlock an electronic device.

- CBP relies on 8 USC §1357(c) and other provisions to authorize a warrantless search of personal effects in the possession of any person seeking admission to the U.S., if the officer has "reasonable cause" to suspect that grounds for the denial of admission exist, which would be disclosed by the search**.**

[4] *See* June 20, 2017 Due Diligence Questions for Kevin McAleenan, Nominee for Commissioner of U.S. Customs and Border Protection (CBP), *available at* www.AILA.org at Doc. No. 17072667 (posted 7/26/17). *See also* AILA Practice Pointer: Rights of LPRs at Ports of Entry, at Doc. No. 17032261 (posted on 3/21/2017).

While the new CBP policy puts into place some additional safeguards with respect to material covered by the attorney-client privilege, the onus remains on the traveler to assert that the material is privileged. Once the traveler asserts that material on the device is privileged, the information on the device must be assessed by a remote team of experts, which presumably involves confiscation of the device.

The Fourth Amendment and the Border Search Exemption

The U.S. Supreme Court has long held that the federal government has the right to conduct random searches of persons and conveyances crossing our international borders under what have been dubbed a "border search exception" to the Fourth Amendment. CBP has interpreted this exception to permit U.S. Customs officers at the ports of entry to conduct warrantless searches, not only of people and conveyances, but also of their electronic devices, including password-protected laptops, phones, and other hand-held devices. These searches are not limited to foreign nationals but can be conducted on anyone crossing the border, including U.S. citizens.

While often referred to as the "border search exception," CBP's right to conduct warrantless, suspicionless searches at the border is not really an exception to the Fourth Amendment, but an interpretation of what constitutes a "reasonable" search. In *United States v. Ramsey*, 431 U.S. 606 (1977), the Supreme Court held that it is reasonable to conduct border searches without a warrant "simply by virtue of the fact that they occur at the border."[5] In another case, the Supreme Court stated, "[i]t is axiomatic that the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity."[6] Indeed, "the Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border."[7] For this reason, the Supreme Court has held that stops and examinations are reasonable in the absence of a warrant or probable cause when they are conducted both at the U.S. border and the "functional equivalent of the border," such as international airports.[8]

Are There Any Exceptions to CBP's Authority to Search Electronic Devices?
III. Are There Any Exceptions to CBP's Authority to Search Electronic Devices?

There are almost no exceptions to CBP's authority to search electronic devices. However, the agency policy does note that where a traveler asserts that the electronic device contains privileged information, such as communications subject to attorney-client privilege, the CBP officer conducting the search "must consult with the local Associate/Assistant Chief Counsel or U.S. Attorney's Office before conducting the examination."[9]

[5] *United States v. Ramsey*, 431 U.S. 606, 616 (1977).
[6] *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004).
[7] *Id.* at 152.
[8] *See, e.g.*, *United States v. Irving*, 432 F.3d 401, 414 (2nd Cir. 2005).
[9] *See* DHS Privacy Impact Assessment for the Border Searches of Electronic Devices (Aug. 25, 2009) at 11, *available at* https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_laptop.pdf

The new directive addresses this concern by outlining procedures when dealing with information which is protected by attorney-client privilege or attorney work product doctrine. The rule provides, in relevant part:

- **5.2.1.1**: The Officer shall seek clarification, if practicable in writing, from the individual asserting this privilege as to specific files, file types, folders, categories of files, attorney or client names, email addresses, phone numbers, or other particulars that may assist CBP in identifying privileged information.

- **5.2.1.2**: Prior to any border search of files or other materials over which a privilege has been asserted, the Officer will contact the CBP Associate/Assistant Chief Counsel office.... Officers will 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.

- **5.2.1.3**: At the completion of the CBP review, unless any materials are identified that indicate an imminent threat to homeland security, copies of materials maintained by CBP and determined to be privileged will be destroyed....

It is too early to determine if these initiatives will ease concerns expressed by the American Bar Association (ABA) over searches of lawyers' laptops at the border.[10] Attorneys should be aware of the privileged materials that they are transporting across the border and should educate their clients on the need to assert the privileged nature of any communications contained on their own devices in the event that they are searched at the border.[11]

I. Preservation of Attorney-Client Privilege

On May 5, 2017, the ABA sent a letter to former U.S. Department of Homeland Security (DHS) Secretary John Kelly and the Acting General Counsel for DHS, Joseph B. Maher, expressing its concern regarding the standards permitting CBP and U.S. Immigration and Customs Enforcement (ICE) to search electronic devices at U.S. border crossings without any showing of reasonable suspicion.[12] The ABA referenced a 1995 case from the U.S. District Court for the Southern District of Texas, in which the Court held that "when a Customs official, in the course of a routine border search, seeks to take the non-routine step of reading the contents of any document over an attorney's objection that the document is privileged, Customs may not read the document without a warrant or subpoena."[13] In its letter, the ABA made several suggestions to protect attorney-client privileged information on electronic devices. For example, the ABA suggested that the CBP and ICE directives be amended to state that laptops carried by lawyers across the border should only

[10] ABA Expressed Serious Concerns with CBP Border Searches of Electronic Devices, AILA Doc. No. 17051062 (Posted 5/5/2017), *available at* http://www.aila.org/infonet/aba-on-cbp-border-searches-of-electronics.
[11] *See* Congressional Research Service, "Border Searches of Laptop Computers and Other Electronic Storage Devices," by Yule Kim (Nov. 16, 2009); DHS Privacy Impact Assessment: "Border Searches of Electronic Devices" (Aug. 25, 2009) for more details.
[12] ABA Expressed Serious Concerns with CBP Border Searches of Electronic Devices, *supra* note 7.
[13] See *Looper v. Morgan*, Civ. No. H-92-0294, 1995 U.S. Dist. LEXIS 10241 (S.D. Tex. June 23, 1995).

be subjected to a routine physical inspection and that privileged and confidential electronic documents on a device should not be read, duplicated, seized, or shared without a subpoena or warrant.[14]

On July 25, 2017, the New York City Bar Association's ethics committee issued a formal opinion identifying some measures for lawyers to take to address their ethical obligations due to the broad CBP search authority at the border.[15] The opinion notes that attorneys crossing the border address the protection of client data at three points, including:

- Before the attorney approaches the U.S. border;
- At the border when U.S. border officers ask to review information on the attorney's electronic device; and
- After U.S. border officers review client's confidential information.

The opinion states that New York Rules of Professional Conduct Rule 1.6(c) requires attorneys to use "reasonable efforts" to prevent the unauthorized access to clients' confidential information, while Rule 1.1 requires attorneys to take reasonable measures in advance to avoid disclosing confidential information if a border officer attempts to search an attorney's electronic device.[16] The opinion emphasizes that while at the border, attorneys should carry identification regarding their status as attorneys and, based on Rule 1.4, attorneys should notify clients of any disclosure of confidential information to a third party during a border search.[17]

Practical Actions and Security Considerations

Some firms are using alternatives to protect information when traveling internationally, such as:

1. Use of temporary or travel laptops stripped of local documents and client information. Traveling lawyers access their documents through a law firm VPN or use cloud-based document storage and other such services.
2. Use of temporary mobile phones devoid of client contacts and other client information. Request clients to use office number while on travel, which is forwarded to the new cell phone number that remains unpublished.

In August 2008, the Canadian Bar Association published a useful practice advisory on how to secure your laptop before crossing the border.[18] The article provides the following suggestions:

---

[14] For a more in-depth discussion regarding cyber security and the ethics of protecting client data, please refer to the AILA Practice Management Committee article, "Cyber Security and the Ethics of Protecting Client Data, posted on July 28, 2016, published on AILA InfoNet at Doc. No. 16072807.

[15] N.Y.C. Bar Ass'n Comm. On Prof'l Ethics, Op. 2017-5, 7/25/17, *available at* http://www.nycbar.org/member-and-career-services/committees/reports-listing/reports/detail/formal-opinion-2017-5-an-attorneys-ethical-duties-regarding-us-border-searches-of-electronic-devices-containing-clients-confidential-information.

[16] *See* New York Rules of Professional Conduct, 22 N.Y.C.R.R §1200, Rule 1.6(c) and Rule 1.1.

[17] *See* New York Rules of Professional Conduct, 22 N.Y.C.R.R §1200, Rule 1.4.

[18] Luigi Benetton, "How to Secure Your Laptop before Crossing the Border," The Canadian Bar Association, August 13, 2008, *available at* https://www.cba.org/Publications-Resources/CBA-Practice-Link/Young-Lawyers/2008/How-to-secure-your-laptop-before-crossing-the-bord.

1. Travel with a bare/forensically clean computer.
2. Use Software as a Service (SAAS) - software housed on the internet.
3. Turn off the computer at least five minutes before reaching the inspection point to bar access to the Random Access Memory (RAM).
4. Back up data before crossing.
5. Use a different user account to hold sensitive information.
6. Use strong encryption and complex passwords.
7. Partition and encrypt the hard drive.
8. Protect the FireWire data port.
9. Clean your laptop or phone when returned.
10. Wipe smartphones remotely.

Other Resources and Tools

The following additional resources and tools may be helpful to practitioners and their clients:

- ***Electronic Frontier Foundation (EFF)*** - EFF offers a "Know Your Rights Guide for Searches of Electronic Devices" available at https://www.eff.org/document/know-your-rights and a resource on "Digital Privacy at the U.S. Border: Protecting the Data on Your Devices and In the Cloud" available at https://www.eff.org/wp/digital-privacy-us-border-2017.

- ***American Civil Liberties Union (ACLU)*** - ACLU provides "A Few Easy Steps Everyone Should Take to Protect Their Digital Privacy" available at https://www.aclu.org/blog/speak-freely/few-easy-steps-everyone-should-take-protect-their-digital-privacy.

- ***Tactical Technology Collective/Front Line Defenders*** - The Tactical Technology Collective and Front Line Defenders created "Digital Security in a Box," the largest online collection of digital security tools and resources, available at https://securityinabox.org/en/.

- ***CBP, Electronic Devices, and Privacy at Ports of Entry*** – AILA webinar discussing changes at ports of entry (POEs) since the November 2016 election, what rights travelers have to privacy, CBP's authority to search passengers' electronic devices, and best practices for advising clients. Additionally, the webinar discusses how the travel bans have affected business travelers, and whether circumstances differ at land POEs versus airports. Available on AILA Agora at https://agora.aila.org/product/detail/3374.