U.S. Customs and Border Protection Updates Policy on Border Searches of Electronic Devices

Date: January 09, 2018

Original Newsletter(s) this article was published in: Blaneys on Immigration: January 2018

On January 4, 2018, United States Customs and Border Protection ("USCBP") updated its official policy on border searches of electronic devices. The new policy directive[1] (the "New Directive") supersedes its prior policy directive (the "Prior Directive), which was issued on August 20, 2009.[2] The New Directive addresses some, but not all, of the issues that arise in relation to border searches of electronic devices.

Background

The United States Supreme Court has previously found that a routine search of any persons seeking admission to the United States (and their personal effects) may be performed without reasonable suspicion, probable cause, or a warrant.[3] This is based on the premise that there is a reduced expectation of privacy associated with international travel.[4]

Nevertheless, it has long been believed by privacy advocates that USCBP's authority to search a traveller's electronic devices should not be exercised in the same manner as a briefcase or suitcase. This is because hand-carried electronic devices now have the capacity to store a very large amount of personal or business information.

Travellers may be prepared to accept a search of their briefcase or suitcase, since the volume of information typically stored therein is relatively insignificant. However, a search of an electronic device gives rise to significant privacy concerns, due to the vast amount of information saved on such devices.

Unfortunately, travellers seeking entry to the United States often do not know their rights regarding USCBP searches of their electronic devices. As a result, they will usually comply with an officer's request for access to their electronic devices, even when the request goes beyond the scope of USCBP's lawful authority.

Revisions to the Prior Directive

Basic v. Advanced Searches

The Prior Directive did not make a distinction between a standard search of an electronic device and a more detailed forensic search. It also took the position that USCBP officers could perform all searches without any specific suspicion that the person who possessed the device was involved in a crime.

The New Directive now makes a distinction between two different types of searches:

a. An "advanced search" is defined as "any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents." Where a USCBP officer has a reasonable suspicion of an activity that violates laws enforced or administered by USCBP, or a national security concern, they may perform an advanced search of an electronic device (with supervisory approval).

b. A "basic search" is defined as "any border search of an electronic device that is not an advanced search." In the course of a basic search, a USCBP officer may, without having any specific suspicion, examine an electronic device and may review and analyze information encountered during the examination. This includes information that is resident on the device and would ordinarily be visible by scrolling through the phone manually (including contact lists, call logs, calendar entries, text messages, pictures, videos, and audio files).

Although this is a significant change from the Prior Directive, it is merely a formal recognition of the Federal Court of Appeals decision in *United States* v. *Cotterman*.[5] In that decision, the Ninth Circuit confirmed that USCBP officers needed reasonable suspicion of criminal activity before they could justify a forensic search of a laptop seized at the border.

Of course, *United States* v. *Cotterman* was only binding in the Ninth Circuit (Alaska, Hawaii, Washington, Oregon, California, Arizona, Nevada, Montana, and Idaho). By incorporating the decision into its New Directive, USCBP has confirmed that *United States* v. *Cotterman* will now apply to all USCBP inspections.

Handling of Passcode-Protected or Encrypted Information

The Prior Directive did not specifically address USCBP's handling of passcode-protected or encrypted information. The New Directive now states that a USCBP officer may request the traveller's assistance in presenting electronic devices, and information contained therein, in a condition that allows inspection of the device and its contents.

Passcodes or other means of access may be requested and retained as needed to facilitate the examination of an electronic device and its contents. However, they may only be used to facilitate the inspection of electronic devices and information resident on the devices themselves. Passcodes and other means of access obtained in connection with a border search must be

deleted or destroyed when no longer needed and may not be utilized to access information that is only stored remotely.

If a USCBP officer is unable to complete an inspection of an electronic device because it is protected by a passcode or encryption, the officer may detain the device pending a determination as to its admissibility, exclusion, or other disposition. The New Directive makes clear that it does not limit USCBP's ability to seek technical assistance, to use external equipment, or take other reasonable measures to render a device in a condition that allows for inspection of the device and its contents. However, supervisory approval is required in order to detain an electronic device, or copies of information contained therein, beyond an individual's departure from the port.

A USCBP officer may detain an electronic device, or copies of information contained therein, for a "brief, reasonable period of time" to perform a thorough border search "as expeditiously as possible." Unless "extenuating circumstances" exist, the detention of devices ordinarily should not exceed five days. However, nothing precludes USCBP from detaining an electronic device for a much longer period by alleging that "extenuating circumstances" exist.

The New Directive does not specifically allege that travellers have a positive obligation to provide a passcode or other means of access to USCBP during a border search; it merely states that USCBP officers may request access and then detain the device for further examination if the traveller does not provide it. This is likely because the law is still not clear regarding whether travellers actually have a legal obligation to provide passcodes or other means of access during a border search.

On September 13, 2017, the Electronic Frontier Foundation ("EFF") and the American Civil Liberties Union ("ACLU") filed a lawsuit against the federal government on behalf of eleven travelers (ten United States citizens and one lawful permanent resident) whose smartphones and other electronic devices were searched without a warrant at the United States border.

The EFF/ACLU lawsuit alleges that that border searches of electronic devices violate the First and Fourth Amendments to the United States Constitution when conducted without a warrant (based on probable cause that the device contains data indicating that the traveler has broken an immigration or customs law). Specifically, it alleges that the recent U.S. Supreme Court decision in *Riley* v. *California* [6]should apply in the border context. In that decision, the U.S. Supreme Court held that, given the significant and unprecedented privacy interests that people have in their digital data, the Police could not conduct warrantless searches of the cell phones of the people who they arrest.

In summary, at the present time USCBP does not clearly have the legal authority to compel travellers to assist them in unlocking an electronic device at the border. Nevertheless, the New Directive makes clear that USCBP officers will continue to ask for passcodes and other means of access in order to inspect electronic devices. It also makes clear that, if the traveller does not

comply, USCBP may detain the electronic device for further examination. The threat of having their electronic device seized, even temporarily, could compel some travellers to cooperate.

The New Directive also does not address the issue of how long USCBP may delay the entry of *a traveller* in connection with the search of their electronic devices. The threat of an extended delay, which may cause the traveller to miss their flight, could also compel some travellers to cooperate.

Finally, if the traveller is not a United States citizen, there are additional tactics that a USCBP could utilize to compel the traveller's cooperation. For example, they could threaten to summarily refuse the traveller's admission to the United States. If this occurs, it may also become more difficult for the traveller to enter the United States on future occasions. The threat of a refusal could compel some travellers to cooperate.

Restrictions on USCBP Access to Information in the "Cloud"

The New Directive formally clarifies the scope of the information that USCBP officers are permitted to access when conducting border searches of electronic devices. It now clarifies that a border search should include an examination of only the information that is resident on the device itself and accessible through the device's operating systems or through other software, tools, or applications. In other words, officers may not use the device to access information that is solely stored in the "Cloud."

Prior to beginning a search, USCBP must take steps to ensure that the electronic device is not connected to any network. In other to avoid accidentally retrieving or accessing information stored in the Cloud, which is not otherwise present on the device, USCBP officers must either request that the traveller disable connectively to any network (i.e. place it in Airplane Mode) or, in certain cases, disable the network connectivity themselves.

This means that information stored on Cloud-based servers (e.g. DropBox, Google Drive, etc.) should fall outside the scope of a USCBP search. Based on this policy, information privately stored in the traveller's social media accounts should theoretically fall outside the scope of a USCBP search as well.

Of course, many applications store synched copies of Cloud-based information on the device itself. If this information remains accessible after the device has been disconnected from the Internet, this means that a local copy has been saved on the device. According to the New Directive, USCBP officers are permitted to examine this information.

Although the formal exclusion of Cloud-based information from a USCBP search is a positive step, it was actually in place prior to the issuance of the New Directive. In a memorandum dated April 13, 2017, USCBP previously clarified that border searches of electronic devices should be limited to information physically resident on the device when it is presented for inspection.

Privileged or Other Sensitive Material

The Prior Directive provided that legal materials, for which attorney-client privilege may be asserted, were not necessarily exempt from border searches but would be subject to special handling procedures. The New Directive now provides additional clarification regarding the specific procedure that USCBP officers must follow when they encounter information that they identified as privileged or over which a privilege has been asserted:

a. If a USCBP officer encounters information identified as, or asserted to be, attorney-client privileged information or attorney work product, the officer must seek clarification from the individual asserting the privilege regarding the specific files, attorney or other client names, or other particulars that may assist USCBP in identifying the privileged information.

b. Prior to any border search of the files or other materials over which privilege has been asserted, the officer must contact the USCBP Associate/Assistant Chief Counsel Office. In coordination with that office, the USCBP officer will ensure the segregation of any privileged material from other information examined during the border search to ensure that any privileged information is handled appropriately.

c. At the completion of the USCBP review, unless materials are identified that indicate an imminent threat to homeland security, copies of materials maintained by USCBP and determined to be privileged will be destroyed, except for any copy maintained solely for the purposes of complying with a litigation hold or other requirement of law.

d. Information determined to be protected by law as privileged or sensitive will only be shared with agencies or entities that have mechanisms in place to protect such information.

The Prior Directive confirmed that other possibly sensitive information (such as medical records and work-related information carried by journalists) must be handled in accordance with any applicable federal law and USCBP policy. It also confirmed that USCBP officers encountering business or commercial information on electronic devices must treat it as business confidential information and protect it from unauthorized disclosure. The New Directive reiterates this prior policy.

Conclusion

Some of the guidance contained in the New Directive is clearly a step in the right direction. For example, the extension of *United States* v. *Cotterman* to inspections occurring outside of the Ninth Circuit is a welcome change. The assertion that information stored in the “Cloud” falls outside the scope of a border search is also helpful, even though it merely reiterates what was already stated in an earlier USCBP memorandum. The additional guidance regarding how USCBP officers should deal with privileged information is also an improvement.

Unfortunately, the New Directive authorizes USCBP officers to request passcode information for an electronic device and to temporarily seize the device if the traveller does not comply. It also

does not address how long USCBP may delay the entry of a traveller in connection with the search of their electronic devices. More importantly, it does not prohibit USCBP officers from threatening to deny admission to foreign nationals who refuse to assist in the unlocking of their electronic devices.

[1] Directive No. 3340-049A, *Border Searches of Electronic Devices* (January 2018).

[2] Directive 3340-049, *Border Search of Electronic Devices Containing Information* (August 20, 2009).

[3] *United States* v. *Montoya de Hernandes*, 473 U.S. 531 (1985).

[4] *United States* v. *Flores-Montano*, 541 U.S. 149 (2004).

[5] 709 F.3d 952 (9th Cir. 2013).

[6] 134 S. Ct. 2473 (2014).