SECURITY AND ADMISSIBILITY CHECKS AT U.S. PORTS OF ENTRY

Regardless of immigration status (e.g., nonimmigrants, immigrants, parolees, U.S. lawful permanent residents, or U.S. citizens), travelers at U.S. ports of entry (and exit), are subject to random search of their baggage. The U.S. Customs and Border Patrol (CBP) considers electronic devices to be baggage, such that cellphones, tablets, laptops, drives, media players, etc. are also subject to search. Searches are conducted pursuant to CBP's immigration, customs, agriculture, and anti-terrorist functions. With respect to immigration, the search can extend to making determinations of a traveler's intentions upon entry, in deciding on admissibility (e.g., a B-1 visitor whose communications indicate an intention to work in the U.S. could be determined inadmissible).

Search of electronic devices

In its border search policy (https://www.cbp.gov/document/directives/cbp-directive-no-3340-049a-border-search-electronic-devices), CBP outlines two categories of search: the basic manual search and the advanced search. In either case, CBP's border search policy provides that the search is limited to information that is locally stored on the device (not the cloud) and that the device can be disconnected from any network (e.g., placed in airplane mode) and will generally be conducted in the presence of the traveler. Travelers will be requested to provide any passwords or disable any security mechanisms in order to facilitate the search. If this request is refused, CBP may detain the device to access its contents. CBP states that passwords will be deleted and destroyed when they are no longer needed.

Basic searches do not require reasonable suspicion and are conducted manually by a CBP officer. Advanced searches can only be conducted when a CBP officer has a reasonable suspicion of illegal activity, or if there are national security concerns, and require supervisor approval. Forensic searches, which involve external equipment being connected to the electronic device to copy or analyze the content, are permitted during advanced searches. During this type of search, CBP may access deleted data, metadata, etc.

If an officer is unable to complete the inspection of an electronic device, CBP can detain the device to perform a thorough search. If this is done CBP will provide a receipt for the detained device. CBP's policy is that the device should generally be detained no longer than 5 days (but it can hold devices longer with supervisor approval). If the CBP determines that there is no probable cause to seize a device or its contents, the copied information is destroyed unless its collection is already authorized.

If a traveler insists that the electronic device contains attorney-client privileged or attorney work product information, the search will continue although in a varied form. First, the CBP officer will seek clarification in writing from the traveler specifying which files/folders/names/email address/phone numbers/etc. contain privileged information. Prior to the search, the CBP officer will contact the CBP Chief Counsel office to oversee the separation of privileged material from other information that will be examined. CBP states that upon completion of the search, all attorney-client privileged information that is deemed to not be a threat to national security will be destroyed. This procedure does not apply to other sensitive information such as medical information or journalists' anonymous sources, but the CBP policy states that it will conduct such searches in compliance with federal law. In regards to business or commercial information, the CBP policy states it will treat this information as business confidential and prevent unauthorized access.

Notably, the Immigration & Customs Enforcement (ICE) also has border search authority, and CBP can transfer detained devices to the custody of ICE. ICE does not provide for the local device (airplane mode) limitation and does not provide for a different procedure for attorney-client privileged information.

Given the extensive information that can be accessed at U.S. ports of entry, travelers should be aware of the extent of their electronic "baggage" and may want to consider traveling with "clean" devices.