Border Searches: Understanding the Risk

Squire Patton Boggs
I. Legal Framework

A. The Fourth Amendment:
   1. Prevents unreasonable searches and seizures, and applies to non-citizens and citizens alike.
   2. Generally requires a warrant, supported by probable cause.
   3. Allows certain exceptions for searches in public.
      a. Reasonable suspicion of danger.

B. A border search is *per se* reasonable, and will not require a warrant.
   1. But highly invasive border searches require reasonable suspicion.
      a. Downloading files is highly invasive, and may require reasonable suspicion.
      b. An ongoing investigation can create a reasonable suspicion.
II. Scope of Border Search

A. Border searches occur at all points of entry, including ports, airports, and roads.

B. U.S. Customs and Border Protection ("CBP") may search persons, luggage, and electronic devices.
   1. CBP can search anyone, regardless of citizenship.

C. CBP generally conducts two types of searches.
   1. A basic search:
      a. Limited to data “ordinarily visible by scrolling through the phone manually.”
         i. Examples include e-mail, text messages, contacts, and photographs.
         ii. If nothing suspicious, the device is returned.
      b. CBP may ask the traveler to enter a password. If the traveler declines, CBP may detain and image the device. There is no fixed timeline for returning the device.
   2. An advanced search (typically where the traveler is connected to an ongoing investigation):
      a. CBP will image and may detain device.
      b. Two requirements:
         i. Reasonable suspicion of a criminal violation, and
         ii. Approval by Supervisory Agent.
III. Limitations on Border Searches

A. Without a warrant, exigent circumstances, or other exception, CBP generally cannot:
   1. Compel a traveler to answer questions.
   2. Physically force a traveler to enter a password. Though one federal court has entertained claims for compelling entry of a password.
   3. Review information “from the Cloud” or privileged documents.
      a. CBP must disconnect networks before the search.
   4. Retain information not related to customs or immigration.
      a. For example, CBP must destroy bank records unrelated to immigration or customs.
      b. But CBP can retain bank records related to an ongoing investigation.

B. Potential Consequences of Non-Compliance
   1. Physical detention for up to 72 hours.
   2. Seizure of luggage and electronic devices, with no firm timeline for return.
   3. Denial of entry to the U.S.
IV. Best Practices

A. Prepare a concise, accurate explanation for your trip.
   1. Avoid ambiguous answers.
   2. Carry your travel visa with you at all times.

B. Ask for an interpreter if necessary.

C. Carry a written list of contacts, containing:
   1. Phone numbers for your employer and any relatives living in the U.S.
   2. Contact information for an attorney.
   3. Consular and Embassy contacts.

D. Carry a temporary smartphone device and laptop computer.

E. If you are represented by counsel in the United States, carry a letter stating that you are represented, and that CBP should direct any questions with legal import to your counsel.