FAQ on Searches of Personal Electronic Devices By Customs and Border Protection Officials

Can Custom and Border Protection (CBP) Officers legally search my laptop, mobile phone, or other personal electronic device?

Yes, CBP officers have broad discretion and authority pursuant to federal statute and regulation to perform any manner of search of individuals and their possessions at ports of entry. Keep in mind that any traveler, regardless of citizenship status or behavior, can be temporarily detained by border agents for more detailed questioning, a physical search of possessions, or a more extensive physical search. These search provisions have been consistently upheld by the federal courts.

Where can I find information about CBP’s searches of these devices?

The Border Search of Electronic Devices Privacy Impact Assessment describes CBP’s practices with regard to search, detention, copying, and seizure of electronic devices, including laptops, cell phones, and digital media. Review [http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_laptop.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_laptop.pdf) for more information.

What should I do if a CBP Officer asks to access my device?

We recommend you provide access to your electronic device if you are asked to do so by CBP Officers. Failure to do so will result in the seizure of the device and possibly your detention for some period of time. Devices that have been seized can take months before they are returned. If an officer is going to search or access your device, don’t take any steps to destroy data or otherwise obstruct that process. Knowingly interfering with a CBP Officer’s investigation is a serious crime. Write down the agent’s identifying information and collect a receipt for property if appropriate.

What should I do if a CBP Officer asks for my passwords?

We have not yet heard of the CBP forcing someone to give up a password for data stored in a secure environment versus the device itself – though this too may change. If a CBP Officer asks for your account password or encryption passphrase, or to decrypt data stored on your device, we recommend that you provide this information. While technically only a judge can force you to reveal information to the government, if you refuse to provide information or assistance upon request, the Officer may seize your device for further inspection or consider you uncooperative, which the agent may take into consideration when deciding whether to allow you to enter the United States.

What types of data or information can I travel with on my device?

We encourage University employees not to carry sensitive information on any electronic devices when traveling overseas.

You should not take with you ANY of the following without first obtaining specific advice:

- Data or information received under an obligation of confidentiality or is otherwise classified.
- Data or analyses that result from a project for which there are contractual constraints on the dissemination of the research results.
- Computer software received with restrictions on export to or on access by foreign nationals.
- Devices or equipment received with restrictions on export to or on access by foreign nationals.
- Private information about research subjects
• Devices, systems or software that was specifically designed or modified for military or space applications.

How do I best protect sensitive information when travelling abroad?

Start a practice of leaving your laptop behind and bringing a ‘clean’ computer that does not include restricted software, data, or other sensitive information. Bring an encrypted memory stick or access information on a secure cloud service at your destination. If transporting sensitive data is absolutely necessary, sensitive data must be encrypted. A convenient alternative is storage of data in a secure cloud environment rather than on a device.

How does export control law apply to my travel if I have sensitive information on my device?

In most cases, if you’re traveling to another country with a university-owned laptop with typical office productivity software, you will probably not need an export license as long as the equipment is always under your immediate control and returns to the US within a year. However, if you are travelling to an embargoed country, or you have non-retail-grade encryption software installed, or the device includes EAR or ITAR controlled data, or if the hardware is unusually sophisticated, you should check with the NC State Research Compliance Office for further advice.

If you are working on a project that involves EAR or ITAR controlled technologies, your device may contain controlled technical data that cannot be shared with foreign parties without a license. You should not take a device with such data outside the US. If you do, it is critical that you inform the Export Control Office if such data may have been compromised while traveling due to the device being lost, stolen, or outside your control.

Do any other laws apply to sensitive information when traveling abroad?

Aside from export control laws, University policies regarding protection of student, financial, sensitive DoD or other research data, and/or FERPA or HIPAA-controlled data may apply to this information. We strongly urge you not to store this data on any device taken outside the US.

Do you have any other general guidance on protecting data or sensitive information when traveling abroad?

• Beyond the export laws, you should also be aware that traveling with electronic devices may result in unexpected disclosure of personal information. Certain countries are known for accessing files upon entry, so you should be extremely careful about any proprietary, patentable, or sensitive information that may be stored on your device. For certain countries, this may include material that might be perceived as pornographic, or culturally inappropriate.
• Just as CBP Officers in the United States, inspectors in other countries may also take possession of laptops or other electronic devices for various periods of time, or permanently depending upon the circumstances. Be wary of bringing a laptop overseas with any financial or other personal information that you would not want viewed without your permission.
• If a laptop is to be used only for making presentations, consider taking a memory stick or storing the presentation on a cloud-based server instead. If you are using a laptop for other purposes (such as email), instead make it a practice to bring ‘clean’ computer that does not include restricted software, data, or other sensitive information.
I heard about a device ban on certain flights to the United States. How will that affect my travel?

The Department of Homeland Security has determined it necessary to enhance security procedures for passengers at certain last point of departure airports to the United States. As part of the enhanced security procedures, electronic devices larger than a cell phone/smart phone will not be allowed to be carried onboard the departing aircraft in carry-on luggage or other accessible property. Electronic devices that exceed this size limit must be secured in checked luggage. Necessary medical devices will be allowed to remain in a passenger’s possession after they are screened.

These security procedures apply to flights departing to the United States from 10 specific foreign airports. The affected airports are:

1. Queen Alia International Airport (AMM)
2. Cairo International Airport (CAI)
3. Ataturk International Airport (IST)
4. King Abdul-Aziz International Airport (JED)
5. King Khalid International Airport (RUH)
6. Kuwait International Airport (KWI)
7. Mohammed V Airport (CMN)
8. Hamad International Airport (DOH)
9. Dubai International Airport (DXB)
10. Abu Dhabi International Airport (AUH)

These enhanced security measures will only affect flights from 10 of the more than 250 airports that serve as last points of departure to the United States, so only a small percentage of flights to the United States will be affected. Airlines will know in advance which flights are affected by these measures, and should remind or provide notice to you of the electronic device ban.

What types of electronic devices will not be allowed to be carried on-board?

The approximate size of a commonly available smartphone is considered to be a guideline for passengers. Examples of large electronic devices that will not be allowed in the cabin on affected flights include, but are not limited to:

- Laptops
- Tablets
- E-Readers
- Cameras
- Portable DVD players
- Electronic game units larger than a smartphone
- Travel printers/scanners

For more information and travel tips, please visit www.TSA.gov.

Will this device ban affect other flights, especially flights to these airports?
No. The device ban does not apply to domestic flights in the United States or flights departing the United States. Electronic devices will continue to be allowed on all flights originating in the United States.