GUIDANCE FOR TRAVELLING WITH ELECTRONIC DEVICES

We are a global university and the mobility of our students, faculty and staff is dependent on the use of electronic devices, *e.g.,* laptops, tablets, smartphones, digital cameras, etc. Our electronic devices hold personal and professional data and are pathways to data stored elsewhere, including the cloud. We risk the release of sensitive personal and university information when we travel.

When traveling internationally, your electronic devices may be subject to involuntary or voluntary inspection, copying of data, or seizure of your device-*regardless of your citizenship or destination*.

BEST PRACTICES

- Travel with fewer electronic devices (laptops, e-book readers, smart/cellphones, tablets, digital cameras, etc.)
- Travel with as little data as possible. Backup business-related data (including photos) to a secure cloud server maintained by your home institution, external drive, or disc before you travel. Personal data should be similarly replicated, perhaps using a service like Dropbox.
- Know whether Export Control limitations are an issue for your device and data. Confer with your office of research compliance.
- Strongly consider leaving your personal devices at home. Instead, purchase or use low-cost loaner tablets and notebooks that are wiped clean of data after travel. Also, pre-paid cellphones are widely available. Most constituent institutions have free loaner programs for university employees traveling on university business.
- Assume that any network, such as a hotel or café wi-fi, is insecure. When using such a network, avoid accessing or entering sensitive information. Keep the security software current on electronic devices.
- Disable any broadcast services, for example Bluetooth, wi-fi, GPS when not in use.
- Do not leave your electronic devices unattended, even in a hotel room, or loan them to others while traveling.
- Encrypt devices, but be mindful that some countries, including China and Russian Federation, forbid the transportation, in or out, of encrypted devices.
- Do not lie to a government official.
- Use unique passwords and change any passwords if used abroad. Don't rely on fingerprint verification alone.
- Power devices down when not needed and particularly going through customs.
- If data is privileged, such as through an attorney-client relationship, declare it to the government officer.
- If you relinquish your device to a government official for further testing, request a receipt.

RESOURCES

https://travel.state.gov/content/passports/en/go/TraveltoHighRiskAreas.html
https://www.cbp.gov/sites/default/files/documents/inspection-electronic-devices-tearsheet.pdf
http://www.americanbar.org/publications/gp_solo/2013/may_june/the_danger_us_customs_searches_returning_lawyers.html
https://www.nytimes.com/2017/02/14/business/border-enforcement-airport-phones.html
http://fortune.com/2017/02/08/social-media-at-the-border-can-agents-ask-for-your-facebook-feed/
http://www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html?_r=1&pagewanted=2&ref=opinion