Best Practices when Travelling to High-Risk Countries

Anyone visiting High-Risk countries, especially China should take precautions to protect the data on their devices such as mobile phones, tablets and laptop computers. Intellectual property and your login/password will be monitored and logged while visiting many of the countries mentioned below.

Plan well in advance. Below are suggested guidelines.

- Travel only with data needed for your trip.
- Consider leaving USB drives behind as they can easily get damaged by magnetic scanners while entering and exiting the airports security screening.

Laptop/Tablet:
- Take a loaner laptop which has all the security updates installed.
- Disable Bluetooth, Camera and Wi-Fi till you have reached your destination. Enable only those features which you need at that time.
- Use strong password or pin to unlock the system. Use a password that is different from any you have used elsewhere. Minimum length should be 8 characters. Use combination of upper and lower case alphanumeric characters, numbers and special characters.
- Do Not Perform Any Personal Banking While On Your Trip!
- Remove all non-essential data before your trip.
- Use of CUIT VPN is to access Columbia University resources only and not for Internet resources. Browsing the Internet or logging into GMAIL or OWA is not available with the VPN. China and Russia have a ban on VPN and encrypted data traffic. Therefore, all data use is monitored, passwords and login accounts are tracked.
- As a rule, check export/import policies for the country you are visiting. In some cases, customs officials will require you to enter password to your laptop, and may take it away for inspection, or hold it. In the latter case, get a document with details of your laptop, and contact the American Embassy.
- Physical control of the device is important. Keep the laptop with you and do not leave it behind in hotel. In any case assume the data has been copied.
- Have the laptop wiped clean on return. The same applies to tablets and other mobile devices.
• Do not backup data and restore to your regular use computer/device. Back it up to an external drive.

Phone:
• Preferably take a pre-paid phone or a loaner.
• If using your regular phone, backup data; **reset phone to factory settings** and prepare only needed information for travel.
• Keep Bluetooth and Camera off. If possible turn off Wi Fi when not in use.
• Shut down the phone when it is not needed.
• Disable all unwanted features and apps.
• Do not plug in your phone to charger kiosks. There may be a computer attached to capture data from the phone.
• Use CUIT VPN to access Columbia University on-campus resources only.
• Always keep the phone with you.
• Wipe out the loaner phone on return.
• Do not back it up and restore data to the regular use phone.

Internet Access:
• While using a VPN to access the Internet is highly recommended, VPN usage is banned in China. However, CUIT recommends using their VPN to access Columbia University on-campus resources.
• Do not send any important data over Wi Fi.
• VPN must be turned off in China to browse the web both on laptop/tablet and phone.
• Skype connections are monitored.
• CU provides VPN access for faculty and staff. Software can be downloaded at https://cuit.columbia.edu/remote-access-services.

Email:
• Gmail/Lionmail is not accessible from China.
• Microsoft Office 365 account is accessible from local China site. Traffic is tracked and unencrypted.
• SIPA IT Recommends creating a new temporary email account at https://outlook.live.com/owa/. Make note of the password as SIPAIT has no access to reset passwords on this account.
• Forward your regular email to the new account for the duration of travel.
• Turn off forwarding upon return from your visit.
• Use a **password** that you have not used for any of your other accounts, including email, personal banking and shopping accounts.
• If the devices are scanned or you are asked to turn over a device, reset password immediately on getting the device back.
Given below is a list of high risk countries.

- Afghanistan
- Algeria
- Belarus
- Burundi
- Cameroon
- Central African Republic
- Chad
- China, The People's Republic of
- Congo, Democratic Republic of the
- Crimea (Region of Ukraine)
- Egypt
- Eritrea
- Haiti
- Hong Kong
- Iran
- Iraq
- Kenya
- Korea, Democratic People's Republic of
- Lebanon
- Libya
- Mali
- Mauritania
- Myanmar
- Niger
- Nigeria
- Pakistan
- Palestine
- Russia
- Saudi Arabia
- Somalia
- South Sudan, Republic of
- Sudan
- Syria
- Thailand
- Ukraine
- Venezuela
- Yemen
- Zimbabwe