**GUIDANCE NOTE FOR PROTECTING ELECTRONIC DEVICES WHEN TRAVELLING TO THE USA**

The US Customs and Border Protection have extensive powers at the border. They have the right to inspect, without a warrant, any person trying to gain entry to the US, and their belongings. More invasive searches require the border officials to have a level of suspicion regarding the individual but the examination of electronic devices (short of forensic investigations) does not require suspicion.

***Before your trip:***

1. Reduce the amount of digital information you take across the border – leave behind devices which are not required
2. Use a temporary device just for your trip if appropriate
3. Delete sensitive/personal data or transfer it securely to the cloud if possible. (But beware of completely wiping your hard drive before travelling as this may attract suspicion)
4. Ensure you use full-disk storage encryption (even for cloud storage)
5. Use a strong password for encryption that is not easy to guess but is memorable to you
6. Ensure all data is backed up elsewhere
7. Ensure your device is turned off when you arrive at the border
8. Talk to your employer in advance if you are taking a work device
9. Start using ‘private browsing mode’ in your web browser in advance to reduce your online forensic footprint
10. Do not try to hide data on your device

***At the U.S. Border***

1. Decide how you will respond to demands prior to your arrival at the border
2. Stay calm and be respectful
3. Do not lie or be physically obstructive
4. If you have any problems, note the name, badge number and agency of the government officials you deal with
5. Avoid implicitly giving consent – if ambiguous, find out whether you are being asked or ordered to unlock your device or provide a password
6. If you are being asked to grant access to your device, you have the option to politely decline (please see the section with options below) – there is legal uncertainty about whether one is legally obliged to grant access to their devices or divulge passwords. Such legal uncertainty allows US border authorities to ask for such access and password details and to issue public statements to the effect that failure to provide information to assist them may result in the detention and/or seizure of the relevant electronic device(s)
7. If your device is accessed, the border official and a supervisor should both be present when possible
8. Searches of your electronic devices should be conducted in your presence unless there are national security, law enforcement, or other operational considerations that make it inappropriate to permit you to remain present. Permitting you to be present in the room during a search does not necessarily mean that you will be permitted to witness the search itself. If permitting you to witness the search itself could reveal law enforcement techniques or potentially compromise other operational considerations, you will not be permitted to observe the search itself
9. Seizure of a device and copies of information is possible – don’t panic - an officer may detain electronic devices or copies of information contained therein with sign off by a supervisor, for a brief, reasonable period of time to perform a thorough border search. The search may take place on-site or at an off-site location, and must be completed as expeditiously as possible. Unless extenuating circumstances exist, the detention of devices ordinarily should not exceed five (5) days. If your device is seized, the officer detaining the device must issue a completed Form 6051 D to you prior to your departure
10. If you are detained for further questioning by immigration authorities, you may not be entitled to legal representation during primary and secondary inspection. Even so, some immigration lawyers recommend that travellers carry with them the number for a legal aid hotline or a specific lawyer who will be able to help them, should they get detained for further questioning at a port of entry. Even if such a lawyer is not able to get into the actual space, they can look to intervene in other ways. Lawyers (who are authorised to practise law in the USA) who fill out a prescribed US form (G-28) on behalf of a traveller headed into the U.S. might be allowed to advocate for that individual, although local practices can vary

**If you are detained, please contact Jon Hancock (Head of Central Secretariat) at (0044) (0)20 7594 5535 (email: jonathan.hancock@imperial.ac.uk) and/or Milena Radoycheva (Head of Legal Services Office) at (0044) (0)20 7594 3251 (email: m.radoycheva@imperial.ac.uk) or, if easier, any other trusted colleague at Imperial College with a request that he/she escalates the matter immediately to the Central Secretariat. Please leave a voice mail on the above numbers if no one picks up the phone at the time you call. The Central Secretariat can then organise for a suitable local lawyer to provide assistance on the ground.**

***What are your options at the US border?***

**Option 1: Comply with an order to unlock your device/ provide password**

* You may choose to inform the border agent that you are complying under protest and that you do not give consent (this may be helpful if you legally challenge the search of your device at a later date)
* You can also inform the border agent if any information they are about to access is confidential information (e.g. business or commercial information) and should be protected from further disclosure. The reason for pointing this out is that officers encountering business or commercial information in electronic devices are required to treat such information as business confidential information and have to protect that information from unauthorised disclosure (as per their own guidance)

*Risks:*

* The contents of your device may be accessed, including cloud content
* Your data may be copied and stored (although if upon further examination there is no probable cause to seize it, any copies of the information should usually be destroyed as expeditiously as possible)

**Option 2: Refuse to comply with an order**

* There is a chance you may be allowed to continue through security

*Risks:*

* The incident may be escalated
* Your device may be seized
* You may find you are subject to increased US border security in the future
* Entry to the US may be denied

**Option 3: Request that the order be withdrawn**

* You may choose to explain that the data is sensitive/ confidential or belongs to your employer and therefore the order should be withdrawn

*Risks:*

* Alerting the border agent to the nature of the contents of your device may not be in your interest

***After you leave the border***

* Change your passwords and login details as soon as possible if you provided these at the border
* Make a note of the incident if you are unhappy about how you were treated as soon as possible and try to identify any potential witnesses
* Inform the College’s Central Secretariat of the incident and, if necessary, seek legal advice via the Central Secretariat