Frequently Asked Questions
Regarding
Inspection of Technical Devices When Traveling

The below guidance was developed via a collaboration by the Offices of IT Security, General Counsel, Research Support, Visa Services, Global Administrative and Travel Support and Export Controls at Duke University. It is intended to provide general advice to those who plan to travel abroad and may encounter questions regarding their technical devices while doing so. This article does not constitute legal advice and should not be taken as such. If you have any questions about your legal status in the United States, we suggest you consult a personal immigration attorney.

Takeaways to Remember:

- Notify OIT security if your password is divulged/accessed by someone other than yourself.
- Check with your departmental IT or OIT for loaner laptops.
- Utilize multi-factor authentication: DUO app and yubikey allow secondary log in passwords without having to be connected to the internet.
- Store your sensitive documents in DukeBox (box.duke.edu).
- Contact ISOS and Global Administrative and Travel Support office if you have a device detained.

1. Can you be asked by a U.S. Customs and Border Patrol Agent or an Immigration and Customs Enforcement Officer to log into, or provide your passwords to, your device and/or to access your applications?

Yes, when you traveling across borders, you and all of your belongings – including IT devices - are subject to search. It is important to note that while you are in transit (i.e., before you have been admitted to the United States or after you have left), the laws and constitutional protections that apply within the country do not apply within border areas. To date, these exceptions to the search and seizure laws have been upheld in court as lawful.

2. Is the inspection of your IT device part of a new policy or law that Customs and Border Patrol (CBP) and Immigration and Customs Enforcement (ICE) agents enforce?

No, the ability of Immigration and Customs officials to search your personal belongings when crossing a border in order to ensure that no violation of U.S. law has occurred is one of the key purposes of a having inspections at the points of entry and exit. With the increase in everyday use of technology by average citizens, the expansion of searches into technological devices traveling with them followed a predictable path. As noted in the "Privacy Impact Assessment" conducted by the U.S. Department of Homeland Security dated August 25, 2009, "With changes in technology over the last several decades, the ability to easily and economically carry vast amounts of information in electronic form has risen dramatically…When these devices are carried by a traveler crossing the U.S. border, these and all other belongings are subject to search by the U.S. Department of Homeland Security (DHS) to ensure the enforcement at the border of immigration, customs, and other federal laws. In particular, U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE) may conduct border searches of such electronic devices as part of CBP's mission to interdict and ICE's mission to investigate violations of federal law at and related to the Nation's borders."

3. How often do searches of electronic devices occur?

While the topic has hit social media venues quite a bit in early 2017 given a few high profile incidents, according to the New York Times, the number of searches are relatively low. In the article, a U.S. Customs agency

spokesman quoted only "4,444 cellular phones and 320 other electronic devices were inspected in 2015 which represented 0.0012 percent of the 383 million arrivals that year." Though the article went on to suggest significantly higher numbers in 2016. (See NYT story at the end of this document.)

4. What should travelers do if they are asked to log into their device or to provide a password so an agent can log into a device or an application?

Each individual should assess the risks and rewards of refusing a request from a CBP or ICE official. For Foreign Nationals entering the United States, non-compliance can be grounds for the denial of entry and deportation. For U.S. citizens or legal residents, it may result in detainment of your device and/or costly delays to you (e.g., missed flights). Duke University recommends travelers share their log in information in order to avoid difficulties that could result from refusal. If you do share your NETID log in information, it is recommended that after the encounter you notify the OIT Security Office at security@duke.edu or via telephone at 919.684.2200 to initiate the reset of your Duke password.

5. What happens to the information on my device during a search?

In most cases, the search occurs and the traveler proceeds on their journey. If you have material on your device that you feel is sensitive or proprietary, it is recommended that you tell the CBP/ICE agent this and ask that they take this into consideration when conducting their search. CPB and ICE officials have the ability to copy what is stored in the memory of your electronic device in order to perform a more in-depth "forensic" review at a later date. According to U.S. law, data copied from your device – if not connected to unlawful activity – must be destroyed. The Department of Homeland Security has stated that data copied from devices will be destroyed within 21-days if no unlawful activity is identified. Nevertheless, it is strongly recommended that travelers consider carrying the least amount of data needed when traveling abroad. Loaner laptops are available through Duke's Office of Information Technology. Please contact 919.684.2200 or security@duke.edu to request such a device.

6. Should I store data differently before I travel abroad?

It is always recommended that data used for Duke teaching, research, or work be stored on a drive that is backed up regularly. Each individual is given their own personal network drive where they can easily store all of their digital data and it is only accessed via NETID and password login. Establishing multi-factor authentication protocol to access data via your IT device is recommended. Further, if the digital data that you typically use includes anything that is considered sensitive or restricted data – such as social security numbers, personal health information, sponsored research or human subject data, particularly data that is subject to U.S. Export Controls – you should contact OIT to initiative a data risk assessment and discuss data storage options prior to going abroad.

In general, it is recommended data be stored in the "cloud" (e.g., DukeBox) and not on the actual device and that travelers remove applications for social media and other accounts prior to border crossings. CBP and ICE agents may ask you if you have accounts with certain social media sites even if they do not see the application on your device. You may still be asked to log in so that they can inspect this data and we suggest the same reward/risk assessment be made as to whether or not you chose to comply with the request.

Frequently Asked Questions
Regarding
Inspection of Technical Devices When Traveling

7. What do I do if they detain my device?

If your device is detained, you will be given a receipt for it. Please do not leave the airport without first having this documentation. Further, it is recommended that you copy or take a photo of the serial numbers from each device that you'll be traveling with and leave a copy/photo with a colleague or family member at home. This is also recommended for travelers in general as the serial numbers are helpful if a device is stolen while a traveler is abroad. Serial numbers help in the identification of the device and tracking in the event that a device is stolen or lost during detainment.

If a Duke-owned device is detained, please contact your IT support person at Duke to report the detainment as well as the Office of Global Administrative and Travel Support (globaltravel@duke.edu).

8. What should I do if a non-U.S. (host country) border agent asks to inspect my device or requests my password/login credentials?

As often happens in the immigration space, travelers may see reciprocal treatment when they reach the non-U.S. destinations. If you are asked for your password or login credentials by a non-US government official, it is again, your right to decide whether or not to comply. Careful consideration should be given to what the risks are should you chose not to comply. If you or your device is detained abroad, we recommend you contact International SOS and/or the Office of Global Administrative and Travel Support at Duke. A follow-up report to the nearest U.S. Embassy or Consulate is also recommended. (If you are not a U.S. citizen, report the detainment to the Embassy/Consulate of your nation.)

9. Is the search of my IT device and social media accounts different than the ban on carrying these on-board the airplane?

Yes, these are two separate policies in practice. The search of IT devices, social media and other accounts for unlawful activity has been in practice since travelers first began carrying their devices across borders. The ban of IT devices – those that are larger than a typical cell phone or those that are not medically necessary - from being carried into the cabin area of an aircraft was announced by the Department of Homeland Security on March 21, 2017 (see the announcement by clicking here). Several major airlines that fly out of airports in the Middle East were told to comply with a new mandate, prohibiting certain IT devices from being transported in carry-on luggage and requiring that they be packed in luggage. See more on this policy at https://hr.duke.edu/managers/memos-updates/2017-03/limits-devices-passengers-traveling-certain-countries

In summary…

By all accounts, traveling in today's world takes patience and a positive attitude. Those attributes will be key if you find yourself in the position of having your technical device inspected. We suggest remaining calm, cool and collected. If you're asked for your password, kindly ask if you can log in to the device or application yourself instead. If your device is taken to another room or connected to another device during the inspection, it is safe to assume the data has been copied and you should make notes of the date, time and encounter. Immediately after sharing your passwords, notify security@duke.edu to reset your NETID password and it is recommended that you reset passwords on social media and other accounts as well. Some commentators have suggested travelers leave devices behind, run down batteries or say they cannot remember their log in passwords. We do not recommend these tactics as they could lead to a more invasive search of one's digital identity.

Frequently Asked Questions
Regarding
Inspection of Technical Devices When Traveling

Duke Resources:

If you're a foreign national employed or studying at Duke and are detained while entering the U.S., please contact the Duke Visa Office at 919-681-8472 or by email at visahelp@mc.duke.edu

If you have travel questions or need assistance with passports, visas, please contact the office of Global Administrative and Travel Support at 919.684.2910 or globaltravel@duke.edu

If you feel your data or device has been breached or if you need guidance as to how to back up your information or would like to request a loaner device for your travels, please contact OIT at 919.684.2200 or security@duke.edu

If you have questions about research data, encryption technology and/or U.S. laws regarding exportation of data, please contact the Duke Office of Export Controls at 919.681.6800 or at export@duke.edu

External resources or articles:

- U.S. Transportation Security Administration: https://www.tsa.gov/
- Department of Homeland Security: Privacy Issues in Border Searches of Electronic Devices https://www.dhs.gov/sites/default/files/publications/privacy_privacy_issues_border_searches_electronic_devices.pdf; Privacy Impact Assessment for border inspection of electronic devices: https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_laptop.pdf
- American Immigration Lawyers Association http://www.aila.org/
- American Civil Liberties Union https://www.aclu.org/, https://www.aclu.org/blog/free-future/can-border-agents-search-your-electronic-devices-its-complicated;
- NYT Feb. 14, 2017 piece entitled "What Are Your Rights if Border Agents Want to Search Your Phone?"
- Stop Fabricating Travel Security Advice: https://medium.com/@thegrugq/stop-fabricating-travel-security-advice-35259bf0e869#.ripl3a80o
- Protect your phone from border guards: http://mashable.com/2017/03/04/what-to-do-with-phone-international-travel/#QZKjxS0zmSqf
- Here & Now: http://www.wbur.org/hereandnow/2017/02/16/border-agent-unlock-phon