Securing Your Devices for Travel

Individuals are facing a growing concern over device searches and reviews at the border when traveling. While the actual number of devices searched remain relatively low, the practice of enforcement at air and land borders have largely increased and resulted in less than ideal scenarios for travelers who are denied boarding flights or had devices confiscated.

Policies and enforcement vary across each traveler and within each Country or location visiting. It's important to note that there is not one perfect solution to securing your devices while traveling, rather you need to evaluate your risk levels and make decisions based on your assessment. Although, there's a lot you can do to minimize your risk and protect yourself or others in the instance you are searched - we're here to help you do that!

Why should you care about securing your device? Everyone holds sensitive information on their devices, whether we realize it or not - our devices are tracking millions of data points about us that can be used to identify issues we care about, political stances, where we've been, and who we're connected with. Your device and the platforms you use contain communication and connections to everyone you're in contact with. If your device is searched or seized you risk putting yourself and others at risk.

Types of Searches

In most cases, there are two types of searches that occur while traveling. A basic search is when an agent takes your device and manually reviews information on it. An advanced search is when an agent connects external equipment to your device and copies all your data. In both cases, an agent can proceed without any reason or on the basis of suspicious activity or violation of a law or national security. Your rights depend on your legal status in the Country you are entering and the laws in the local area you are arriving.

Know Your Rights

Cities, States, and Countries can have different laws regarding searching and seizing devices. For example, in the United States - some States require officers to have a warrant to seize or review a device, whereas some do not. Before traveling, review the local laws for where you are traveling and be aware of your rights depending on where and how you are entering.

If you are a citizen of the Country you are entering, you have the most rights at the border as officers cannot legally prevent you from entering the Country but they can seize your devices if you refuse to co-operate or if they think they have grounds for seizure. In what is often determined as a no-win situation, even if you exercise your rights as a citizen and refuse a search this can have unintended consequences for future travel as well. Individuals who are a

permanent resident, visa holder, or tourist have even less rights at borders and failing to comply with demands can result in a denial of entry or worse.

Understanding Your Risk

A risk analysis can help determine the level of precaution you should take at the border. A low risk means that you are less likely to face issues at borders or be subjected to additional screenings but it doesn't mean you shouldn't take the basic steps to protect yourself. A high risk means that you might be more likely to be searched when traveling and reviews or seizures of your devices could put you and others at risk.

When understanding your risk, ask yourself these questions:

- What is my legal status in the Country I am visiting? Am I a citizen or a permanent resident or a visa-holder, or a tourist?
- Are people with my identity - race, religion, sexuality, gender, among others - currently being targeted in the Country that I am entering?
- Does my profession or those that I work with increase my risk at the border? Does access to my device impact others I work with or would it release confidential information?
- Have I traveled to certain countries that are connected to terrorism, drugs, or trafficking and could be scrutinized or flagged by agents?
- Do I have a prior conviction or been under suspicion of committing a crime?
- Am I a public figure or do I hold a position of power among certain groups?
- Have I done activism or organizing that would be viewed negatively by or goes against opinions of the administration?
- Have I spoken out or made public/private comments against the administration and their practices or laws?
- Do I have any reasons to believe I might be more of a target than others entering the Country?

The more times you answer yes to these questions, the greater your risk increases. Whether you determine you are low, medium or high risk, it's important to secure your devices so in the instance of being searched you and your communities are protected.

How to Secure Your Devices While Traveling

Remove Biometric Logins
Disable Face ID and fingerprint recognition on your devices and replace with a strong password. While these are convenient features, they do not offer the same security as a strong password. In some cases, an officer can't force you to disclose your password but they can use your biometrics to unlock your phone without your consent. It's important to choose a long, unique, and hard to guess password as it will make it harder to access your device in the instance your devices are seized.

Power Down Your Devices
Turning off your devices before arriving at border checkpoints provides an additional layer of security which can protect your device against any attacks that attempt to get access to data. Additionally, powering off allows your device to maintain its built-in encryption that is only enabled before you input your password after a reboot.

Clear Your Browser, History, And Data
If you do not want anyone to have access to the data on your device, the easiest way to prevent this is to clear data on your device. Forensic recovery, a tool used by agents, can recover recently deleted data so this isn't fully protective in an advanced search. If you are worried about someone accessing your data, you should enable a factory reset to the device to clear the data entirely. To prevent data being stored on your device while browsing, use private browsing mode to reduce your forensic footprint.

Backup Your Device And Accounts
Create a backup of your data that you leave at home, such as on a hard drive, or can access online, through a cloud service. This also allows you to delete data without the fear of losing it completely.

Logout or Delete Accounts and Apps
You can also logoff or (temporarily) delete accounts that you don't want anyone to look at. Examples include personal or work emails, documents or drives, social media accounts, instant messaging apps or channels, among others. Be sure to backup these accounts before deleting so that once you've entered a Country you can re-download them with your data intact.

Clear Communication And Social Apps
In some cases, agents can request information on your social accounts or even ask for your login details to review private content. So whether or not you have deleted them, it is still important to remove any content you don't want found on the platforms. Minimize or delete any content that would be scrutinized by agents or any chats or groups that put others at risk.

Use A Temporary Device or Leave It At Home
Some individuals might feel more secure by leaving their devices at home while traveling or using a temporary device with limited information. While this is the most secure option when traveling, it can raise suspicion to have completely cleared devices so be sure to add basic apps or info on it.

Install A VPN
A Virtual Private Network (VPN) helps to scramble your location and history on a device. When using a VPN, your device records less data and makes it harder when seized to capture details of your online history and physical whereabouts.

Create A Safety Plan
Create a safety plan with a couple contacts who are aware of your travel, including who to contact in an emergency. Stay in touch with your safety buddies as you enter a Country and create code words or phrases that allow you to communicate with them without disclosing specific details. It can also be helpful to print or write down your travel details and include emergency numbers or contact details in case your devices are seized.

Additional Notes

- Stay calm, respectful and avoid any escalations when being searched or questioned at borders
- If asked to unlock your device, ask to input your password
- Ask to be present for the search of your device
- Do not lie or physically interfere with agents at the border
- Know the different between being requested to do something versus being required, officials at the border often persuade individuals to give consent to searches without being aware of their rights
- Take note of officers name, badge numbers, details of equipment, custody receipt, and any details you can remember

Device Checklist

Remove biometric logins such as Face ID and fingerprints	🟢
Power down your devices before going through security and after landing, before exiting the airport	🟢
Use a long and unique password to lock your phone	🟢
Clear your browser	🟢
Backup your devices and accounts	🟢
Upload sensitive content to an external drive or the Cloud and remove it from the device	🟢
Clear your ‘recently deleted’ or ‘trash’ folders on your devices	🟢
Log out or delete any accounts with sensitive information	🟡
Remove or delete content from communication and social media sites	
Be aware of what content you post or message before, during, and after travel	🟡

Print or write out your travel information (flight, accommodation, etc.) and emergency numbers	🟡
Discuss protocols and practices with your employer if traveling with a work-owned device or on a work-related trip	🟡
Install and use a VPN	🟡
Encrypt your laptop and mobile device	🔴
Avoid bringing sensitive documents or materials on your trip	🔴
Leave your devices at home or use a temporary device	🔴
Back up your device, apply a factory reset and only add back necessary info	🔴
If you choose to decline searches of your devices, prepare for the potential of arrival without your device	🔴

🟢 Low-Risk
🟡 Medium-Risk
🔴 High-Risk

—------

This resource is not meant to replace or supplement legal counsel. If you are worried about yourself and your devices when traveling, consult a lawyer for advice on your individual situation.