Global Engagement Technology Guidance for International Travelers

Introduction

When planning international travel, it's important to consider how you can securely access information from your devices. Not only are the risks of technological breaches multiplying, but many countries (including the United States) are expanding and enforcing laws about crossing borders with technology, and having or sharing content on computers or online. Citizens and non-citizens are subject to such laws.

This guide summarizes best practices to ensure your data is protected before, during, and when you return from your travel abroad. Adhering to the guidelines below can help you keep personal and SCU data secure, and prevent you from transgressing local laws. *Contact associateprovostglobal@scu.edu with any questions.*

What Faculty and Staff Should Do Prior to International Travel

What to pack? In terms of devices, bring only the equipment needed to do your work- if you can travel without the device, don't take it. Start preparing weeks in advance of your trip.

Below you'll find device recommendations that range from best, most secure options to the minimum required actions that help keep devices secure and your data protected.

Best: Travel light

- **Borrow a laptop from SCU.** If you're traveling to a country that has high cybersecurity or privacy concerns, the SCU Information Services Office (ISO) strongly recommends that you leave your current devices behind and travel with a SCU loaner laptop. You can borrow a laptop in place of your own computer. The loaner device will allow you to manage email, view your calendar, run presentations, edit documents, and connect to university websites. The devices are wiped when you return.

- **Connect through Virtual Private Network (VPN).** Download and install SCU's Virtual Private Network (VPN). This will allow you to securely connect to Santa Clara's network as if you were on campus. Be aware that in certain high-risk countries, such as China, the use of the SCU VPN may be illegal, and therefore may not be used. Make sure that you test your ability to get to your data using VPN from some place off campus before leaving.
- **Leave the mobile phone at home.** Consider whether you can travel without your mobile phone, and if you can get by with a Wi-Fi-only device, like an iPad. If the trip is short or to areas with higher risk ratings, the best security option is to travel without your mobile phone. For two-step authentication, you can use the Duo Mobile app on an iPad or a security key - no network or cellular connectivity required.

Good: Travel with less data

- **Bring a new or wiped laptop.** If you cannot travel without a full laptop, another option is to take a new or freshly wiped machine and load only the data you'll need for this trip.
- Whenever possible, leave USB drives at home. These are easily lost and easily corrupted. If you must travel with a USB device, be sure that it's encrypted. Note, some countries (China, Israel, Russia) have restrictions on the import and use of encryption tools and do not allow them with a license or at all.
- **Get a temporary mobile device.** For mobile devices, borrow a device in the country, use an unlocked phone with a local SIM card, or rent/buy a phone at the airport or hotel when you arrive.

Minimum: Travel encrypted

If you must take your own personal device(s), encrypt them and be sure to follow these additional steps before you go. Enable Full-Disk Encryption(FDE) on all your devices for added security. Use strong passphrases instead of simple passwords. *Again, some countries (China, Israel, Russia) have encryption import restrictions.

- Apple devices: Turn on Filevault.
- Windows has a built-in encryption tool called "BitLocker"

Backup your information. Backup your contacts, photos, videos and other mobile device data onto another device or in the cloud. Using a cloud service will keep data you leave behind available to you, provided you can find a secure connection.

Laptops:

- Leave sensitive data stored securely on SCU servers and access it remotely only via SCU's Virtual Private Network (VPN).
- Make sure all operating systems and applications are updated and patched before leaving for your trip.
- Uninstall unused and unnecessary applications and turn off unneeded services on your computer. Leaving them installed and/or running only serves to provide additional, possibly "unlocked" doors for intruders to gain access through when attacking your device.

- Don’t accept any patches or updates while in foreign countries, as infected updates are becoming a more common attack vector.
- When you return, save the documents you created while traveling to another device, completely wipe your computer, and restore it from the backup made before your travel.
- Only connect to known and trusted networks.
- If you have a personal laptop and have multiple accounts (like an administrator account and a non-administrator or “standard” account), use the non-administrator account as your primary user account. The computer will be less likely to allow software (malware) to be installed without you clicking “install” and typing in your administrative password.

Mobile devices:

- Encrypt phone by enabling screen lock (with PIN).
- Enroll it in an international rate plan to avoid incurring exorbitant roaming charges.
- Set up the "find my device feature" on all your devices. This will help you find your phone, tablet or laptop if you lose it and might allow you to disable or wipe data from it if it gets in the wrong hands.
- Consider removing social media platforms or archiving social media posts and texts that could be flagged/seen as anti government.

While Abroad

Always keep your devices with you—either in your hand or in a bag you’re holding. Never leave them unattended, place them in checked luggage, or leave them on the floor beside you. If your device is ever taken out of your sight or confiscated, assume it may have been compromised and have it inspected and cleaned right away.

Bear in mind, thieves often target travelers. Meal times are optimum times for thieves to check hotel rooms for unattended laptops. If you are attending a conference or trade show, be especially wary: these venues offer thieves a wider selection of devices that are likely to contain sensitive information, and the conference sessions offer more opportunities for thieves to access guest rooms

Wi-Fi

- **Avoid Wi-Fi networks whenever possible.** Especially when traveling internationally; in some countries they’re controlled by security services. In all cases they are insecure.
- **Turn off "join wireless networks automatically."** Always manually select the specific network you want to join, only after confirming its name and origin with the provider. Turn off wireless and Bluetooth, when not actively being used.

Laptops

- **Clear your browser after each use**: delete history files, caches, cookies, URL, and temporary internet files.
- **Don’t use thumb drives** given to you, as they may be compromised.
- **Be aware** of who's looking at your screen and shield passwords from view.

Mobile Devices

- **Keep it locked.** Get into the habit of locking your device when you are not using it. Require a strong password to unlock it – not a PIN or swipe pattern – whenever possible.
- **Beware public charging stations.** Many modern mobile charging cables and ports double as data ports. Do not physically connect your mobile device to anything you do not control.

Returning to the U.S.: Electronic Device Searches at U.S. Ports of Entry: What You Need to Know

Travelers need to take precautions and know their rights when re-entering the US, especially depending on the traveler's legal status in the US.

U.S. Customs and Border Protection (CBP) has the authority to search electronic devices—including phones, laptops, tablets and other electronic devices—of anyone entering the U.S., including U.S. citizens and non-citizens. These searches can happen at U.S. land crossings, airports, seaports, and even at CBP preclearance locations abroad, such as Dublin or Toronto. These searches can occur without a warrant or suspicion, which could be a basic search, where the officer reviews the contents of the device, or an advanced search where they connect a device to external equipment to review/copy content.

Conduct a personal risk assessment – which should include your immigration status, travel history and what data you might have on your phone. There's not a one-size-fits all solution because data that may seem sensitive to some may not be to others, depending on your circumstances. That assessment might affect your calculus of whether to push back if CBP attempts to search your phone, for instance, or how much you want to lock down your devices before heading to the airport.

Social Media Content: As of April 9, 2025, U.S. Citizenship and Immigration Services (USCIS) will check for antisemitic social media posts and can use this as a reason to deny immigration benefit requests, such as revoking an international student visa.

- **Privacy Risks:** U.S. Customs and Border Protection (CBP) officers have the authority to search electronic devices, potentially accessing personal, confidential, and sensitive data.

- **Legal Considerations:** At U.S. borders, your constitutional protections are limited. CBP can inspect your devices without a warrant or probable cause, though they are generally restricted to data stored directly on the device and not data stored in the cloud.

- **Possible Consequences:** Refusing to provide access to your devices may lead to their seizure. While U.S. citizens cannot be denied entry for non-compliance, devices may be detained and subjected to further examination. Your travel may also be delayed.

Non-citizens, including visa holders, have fewer rights at the border and may face denial of entry into the United States if they refuse to comply.

Device Recommendations (laptop/phone):

- Turn Off Devices Before Border Crossing: Power down your devices completely before reaching the border to help protect against potential remote access attacks and data interception.
- Limit Cloud Access: The border search will only examine information on the device at the time of the search and cannot access information stored remotely.
- Sign out of sensitive apps, disable automatic logins, and consider removing apps that store personal data. Additionally, you may consider using a VPN for electronic devices.
- Consider removing any specific texts, apps, photos, etc. that you feel are sensitive or wouldn't want a government agent to see.
- Inspect Devices Upon Return: If your laptop is confiscated and later returned, boot it using an external drive and perform a thorough scan for any unauthorized software or changes.

Adhering to these practices can help protect your data and navigate laws when traveling internationally. Read more about how to protect your data at the border and how to handle interactions with U.S. Border Agents.

Returning to SCU

- Change all passwords to any accounts accessed during travel immediately. Assume all internet traffic, including passwords, have been intercepted.
- Save your data and use SentinelOne antivirus to scan devices for malware upon return.
- Restore devices to their pre-travel configuration. This includes all devices you took with you (computers, tablets, mobile phones, etc.).
  - Before reconnecting to campus systems, turn off any travel-specific services, apply any patches released during your absence.

Technology Considerations When Traveling to High Cyber Risk Locations

Travel to locations with different laws and expectations presents distinct challenges to the confidentiality of University data. The U.S. government has identified pervasive threats to information security from certain countries deemed as high cyber risk and privacy locations, for example: Hong Kong, China, Cuba, Iran, Syria, Ukraine, etc., and in these locations there can be no presumption of privacy. This means that travelers should assume all data is accessible by local government and non-governmental actors and that files and information on your devices such as laptops and phone can be compromised, even while they are in your possession. Indeed, SCU has examples from our travelers in which this has happened. SCU advises travelers:

   1. Travel with electronic equipment (laptops, tablets, phones) that are cleared of any data (including news articles, emails) that may be deemed harmful or counter to destination countries national security interests; that contain sensitive information regarding university business, operations and PII, and that limit data carried to only those items necessary to travel and conduct relevant business/research in destination
   2. Enable two-factor authentication and use Duo to access all SCU resources. Operate mindful that all electronic communication is subject to monitoring and extraction; be careful not to discuss politically sensitive topics or share unprotected sensitive information by phone, email or other electronic means.
   3. Do not accept electronic gifts, including USB devices, including from apparently benign sources.

4. Always keep your mobile devices and laptop with you.

China: a special travel situation

Travelers to the People's Republic of China have experienced various issues, including the following:

- Access to services we take for granted, like Gmail and other Google apps, Wikipedia, and Yahoo Mail, are often blocked or filtered.
- The government may monitor Skype connections.
- Individuals using VPNs reported that they are often cut off for hours.
- Hotel staff and government officials can access hotel room safes, so don't expect that a computer or mobile device in a hotel safe will be secure.

Considerations:

- Review the Department of State China Travel Advisory.
- Social Media: Social media accounts are widely monitored in the PRC. Local authorities may use information they deem critical, controversial, or that might involve illegal activity against both the poster of the material and the host of the social media forum under local law. Individuals have also been held responsible for the content that others place within social media spaces they control, such as the comments section under a post or within a group chat that an individual controls.
- Only authorized VPNs are legal in China, and the SCU VPN or a personal VPN is *not authorized*. Both may violate the law and are not recommended.
- Be aware that all texting, messaging and use of WeChat on personal or employer issued phones is monitored. Do not send private messages on government or political topics. It can be difficult to navigate in some places without using WeChat for some forms of communication or payment.

Export Control Management

When traveling internationally with technology, it's important to understand export control laws. Certain technologies, software, and data are restricted and may require a license for export. Ensure compliance with regulations set by your country, such as the U.S. Export Administration Regulations (EAR) or the International Traffic in Arms Regulations (ITAR). Before traveling, please review the SCU Export Control Management website.

The Office of Foreign Assets Control (OFAC) is part of the United States Treasury Department. OFAC manages the United States government's sanctions and embargo programs, as well as the Specially Designated Nationals (SDNs) and Blocked Persons lists. Please reference OFAC's Sanctions Program and Country Summaries for the most current sanctions.

Do not travel to conduct research or educational activities to embargoed countries without first checking with the Research Compliance & Integrity to secure a license from the Department of Treasury, Office of Foreign Assets Control. Any questions regarding export controls should be directed to the Office of Research Compliance and Integrity: (408) 554-5591.

Q&A:

What should I do if my device is confiscated?

- Obtain the name and title of the individual confiscating your device.
- Obtain a “receipt” or comparable written documentation that describes the device confiscated, under what authority, for what purposes, by whom and whom to contact regarding return of the device.
- If your device contains PHI, let the agent know that you are affiliated with Santa Clara University (clinician, researcher, student, etc.) and have HIPAA-protected health information on the machine.

Can I be forced to disclose the password to an electronic device at the U.S. border?

This likely depends on the type of password. You have a constitutional right to remain silent, and it would likely violate your constitutional rights if a government agent compelled you to verbally disclose your password to a device. However, some courts have concluded that the government may compel you to provide a fingerprint, or even force you to apply your own finger to a phone to unlock it. The distinction is that verbally providing your password is considered compulsion of your “testimony,” while the physical act of providing a fingerprint is not “testimonial” and, therefore, is not protected by the Fifth Amendment. You should assume that CBP will ask you to unlock or decrypt any device that you bring to the border and that CBP may assert authority to detain the device itself.

Resources:

National Counterintelligence Executive's Travel Security Tips

Federal Trade Commission Consumer Advice: Online Privacy and Security

U.S. Department of State Country Guides

CISA's Cybersecurity while Traveling Tip Card

Last reviewed and updated 5/7/2025 by the International Travel with Technology (ITT) Working Group:
Nancy Cutler, Deputy CIO for Academic Technology
Kristen Dietiker, Chief Information Security Officer

Staci Hagen, Director of Global Health, Safety and Risk
Susan Popko, Associate Provost for International Programs
Ester Pham, Director of Research Compliance and Integrity
Eric Tillman, Associate Provost for Research