Tech Security While Crossing Borders

Planning Ahead: Before Your Trip

Minimize What You Carry

- **Leave devices at home** when possible - border agents cannot search what you don't bring
- **Use a temporary "travel" device** with minimal data loaded on it
- **Remove sensitive information** from devices you must bring
- Consider which apps you actually need - fewer is better

Backup Everything

- **Make complete backups** of all devices to encrypted storage (leave at home)
- Ensure cloud backups are current and accessible remotely after crossing
- Document device serial numbers for insurance/tracking purposes
- **Remember:** You may need to factory reset devices, so backups are critical

Protect Data You Carry Over the Border

Encryption (Most Important)

- **Use full-disk encryption** on all devices (FileVault for Mac, BitLocker for Windows, built-in for iOS/Android)
- Encryption makes data unreadable without your password
- **Create a strong password for your devices:** Use 4-6 random words or a long passphrase (12+ characters)
- **Do NOT rely on biometric locks alone** (fingerprint, Face ID) - use strong passwords or PINs

Power Off Your Devices

- **Turn off all devices completely** before reaching the border (don't just sleep/lock them)
- This protects against sophisticated attacks that only work on powered-on devices

- Powering off also forces password entry rather than biometric unlock

Additional Preparations

- Log out of cloud services and apps you won't need during travel
- Clear browser history and remove saved passwords
- Consider temporarily uninstall messaging apps
- Consider making social media profiles temporarily private

At the Border: Know Your Rights

Your Legal Status Matters

U.S. Citizens:

- Cannot be denied entry to the U.S. for refusing to unlock devices or provide passwords
- However, refusal may result in device seizure, extensive questioning, and significant delays
- You have the right to remain silent and cannot be compelled to answer questions about religion or political beliefs

Lawful Permanent Residents (Green Card Holders):

- Generally cannot be denied re-entry for refusing to unlock devices
- However, agents may raise questions about your continued status as a resident
- Do not give up your green card voluntarily

Foreign Visitors (Visa/VWP travelers):

- May be denied entry for refusing to unlock devices or provide passwords
- Face the highest risk of consequences for non-compliance
- Should carefully weigh risks before traveling with sensitive data

What Border Agents Can Do

Legal Authority:

- Border agents claim authority to search electronic devices without any suspicion
- They can demand that you unlock devices, provide passwords, or disclose social media information
- They can seize devices for extended examination (days, weeks, or months)

Important Legal Developments:

- A 2019 federal court ruled that suspicionless searches of electronic devices may be unconstitutional
- However, current CBP policy still allows searches without individualized suspicion
- Legal protections continue to evolve - this is contested territory

If Asked to Unlock Your Device

Basic Rules for Everyone:

1. **Stay calm and respectful** - getting emotional may escalate the situation
2. **Do not lie** - lying to federal agents is a federal crime
3. **Do not physically interfere** - comply with demands to hand over devices
4. **Document everything** - try to note agent names, badge numbers, and what was accessed

Your Options:

Option 1: Comply

- If you unlock your device, agents can search all content and make copies
- Consider stating you are complying "under protest and without consent"
- Request that searches be conducted in front of a supervisor

Option 2: Decline

- Politely ask whether they are *ordering* or *requesting* you unlock the device
- If it's a request, you can decline
- If it's an order and you refuse:
  - **U.S. Citizens:** May face device seizure, delays, additional questioning, but cannot be denied entry
  - **LPRs:** Similar to citizens, but may face immigration status questions
  - **Foreign visitors:** May be denied entry to the U.S.

If Your Device is Seized:

- Request a receipt (Customs Form 6051D) documenting what was taken
- Ask when you can expect the device to be returned
- Do not expect quick return - devices may be held for months

Special Considerations

Attorney-Client Privilege:

- If you're an attorney carrying privileged communications, inform agents

- CBP policy requires agents to consult their legal office before searching privileged materials
- However, this is not a complete protection

Journalists:

- Protecting confidential sources is critical
- Consider not traveling with sensitive source information
- Document any attempts to access source materials

Cloud Data:

- CBP policy (as of 2017) states agents should only search data "physically resident on the device"
- They should not use your device to access cloud content
- However, enforcement of this policy is unclear
- If asked for cloud account passwords, you can decline (but face consequences noted above)

Social Media:

- Border agents may ask for social media identifiers/handles
- They may ask to see social media content on your phone
- Foreign visitors on Visa Waiver Program are asked to "voluntarily" provide social media identifiers

After Crossing: Post-Travel Security

Immediate Actions

- **Change all passwords** if you unlocked devices for border agents or provided passwords
- Review account activity logs for unauthorized access
- Check devices for new apps, configuration changes, or suspicious files
- Enable 2FA if it was disabled for travel

Device Inspection

- Consider devices potentially compromised if seized or extensively searched
- Have IT staff conduct security inspection if you have organizational support
- For highly sensitive situations, wipe device and restore from backup

Documentation and Reporting

- Write down everything that happened as soon as possible
- Note all agents involved (names, badge numbers, agencies)

- **If your rights were violated, contact:**
  - EFF at borders@eff.org
  - ACLU for civil rights complaints: https://www.dhs.gov/file-civil-rights-complaint
  - Your organization's legal counsel

High-Risk Travelers: Special Precautions

Journalists, Attorneys, Healthcare Workers, Activists:

- You have professional obligations to protect confidential information
- **Strongest protection:** Don't bring sensitive data across the border
- Access via secure cloud connection after clearing border
- Use burner devices with minimal/no sensitive data
- Ship devices separately (though they can still be searched)

Organizations Should:

- Establish clear travel security policies
- Identify which roles require burner devices
- Provide temporary travel devices when needed
- Create protocols for accessing sensitive data remotely after crossing
- Have incident response procedures for device seizures

Resources

Official Guides:

- EFF's Digital Privacy at the U.S. Border: https://www.eff.org/wp/digital-privacy-us-border-2017
- ACLU Know Your Rights: https://www.aclu.org/know-your-rights/what-do-when-encountering-law-enforcement-airports-and-other-ports-entry-us

Tools and Services:

- Full-disk encryption: FileVault (Mac), BitLocker (Windows), built-in (iOS/Android)
- Password managers: 1Password, Bitwarden
- Secure deletion tools: See EFF's Surveillance Self-Defense guide
- Cloud storage: Consider services with client-side encryption like Tresorit

File Complaints:

- CBP: https://www.cbp.gov/contact/ports
- DHS Office of Civil Rights and Civil Liberties: https://www.dhs.gov/file-civil-rights-complaint
- Traveler Redress Inquiry Program (TRIP) if you believe you're on a watchlist: https://www.dhs.gov/dhs-trip

---

Revision #6
Created 6 November 2025 19:21:34 by Josh
Updated 7 November 2025 15:10:42 by Josh