BUHLER THOMAS LAW
ATTORNEYS-AT-LAW

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

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.

Types of Searches

- A basic search is any border search of an electronic device that generally involves an officer reviewing the contents of the device manually without the assistance of any external equipment.
- An advanced search is when an officer connects external equipment to an electronic device to access to the device, as well as to review, copy, and/or analyze its contents. CBP must have a reasonable suspicion of a violation of law or a national security concern and pre-approval of a senior manager before conducting an advanced search.

Why This Matters to You

- Privacy Risks: CBP may access personal, confidential and sensitive data.
- Legal Considerations: Your rights are limited at the border, but you can take steps to protect your data.
- Possible Consequences: If you refuse to provide access, your device may be seized. Visa holders may be denied entry to the United States if they refuse to provide access. At preclearance locations, this may result in boarding being denied.

Ten Smart Steps to Protect Your Data at the U.S. Border

1. Travel Light: Carry only necessary devices. Consider using a dedicated travel device with minimal personal data.
2. Back Up Before You Go: Save important files securely in the cloud or an external drive before traveling. Keep backups separate from your laptop.
3. Prioritize Password Security: Secure devices with unique, complex passwords. Although fingerprints and other biometric locks offer convenience, they are generally considered less secure than strong passwords. Enabling two-factor authentication (2FA) whenever possible can provide an additional layer of security.
4. Know Your Rights:

- You are not required to share your password, but refusal may lead to device seizure. Visa holders may be denied entry to the U.S. if they refuse to provide access. At preclearance locations, this may result in boarding being denied.
- U.S. citizens can refuse to answer questions beyond identity and travel details, though this may cause delays. Lawful permanent residents cannot be denied entry but may face additional scrutiny. Visa holders may be denied entry if they refuse to answer questions about their trip and visa status.

5. Document the Search: Write down details of the search, including the names and badge numbers of CBP agents. Document the questions they ask. If your interview was recorded, ask for a copy of the transcript.
6. Minimize Stored Data: Carry less data across the border. Consider traveling with a laptop free of sensitive data or apps that collect and store sensitive data. Securely delete files instead of just moving them to the trash. Think about leaving your usual phone at home and buying a temporary phone, then transferring your SIM card or getting a new number at your destination.
7. Encrypt Your Devices: Enable full-disk encryption on all your devices for added security. Use strong passphrases instead of simple passwords.
8. 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.
9. 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.
10. 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.

How to Handle Interactions with U.S. Border Agents

- Be Honest: Never lie to CBP officers.
- Stay Calm: Do not argue or interfere with an inspection.
- Understand Inspection Authority: Understand that CBP has the authority to physically inspect electronic devices. While you are not required to provide your passwords, refusing to do so may result in possible consequences, such as device seizure or denial of entry.

For more information, read this short guide from **Electronic Frontier Foundation's Border Search Pocket Guide.**

If you have questions about traveling to the United States, please contact your immigration lawyer. If you do not have an immigration attorney, you can find a licensed attorney at **www.ailalawyer.org**.

This flyer is intended for general information purposes only and does not constitute legal advice. You should not act or rely on any information in this flyer without seeking the advice of a competent, licensed immigration attorney.