MINAMI TAMAKI LLP
Attorneys at Law

Electronic Device Searches at U.S. Ports of Entry

U.S. Customs and Border Protection (CBP) has the authority to search electronic devices including cellphones, laptops, tablets, and other electronic devices of anyone entering the U.S. regardless of their citizenship status. Searches can happen at airports, seaports, land border crossings and preclearance locations abroad such as certain airports in Canada and Dublin. These searches can occur without a warrant or reasonable suspicion.

Types of Searches

- Basic Search
  - This general involves a CBP officer reviewing the contents of electronic devices manually without the assistance of any external equipment.

- Advanced Search
  - When an officer connects external equipment to an electronic device to access 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 preapproval of a senior manager before conducting an advanced search.

Concerns

- Privacy Risks: CBP may access personal, confidential and sensitive data.
- People have limited rights at the border.
- If you refuse to provide access, CBP can seize your device. Foreign nationals can be denied entry to the U.S.

Tips

- Travel light: Carry only necessary devices. Consider using a dedicated travel device with minimal personal data.
- Back up before you travel: Save important files securely in the cloud or an external drive before travelling. Keep backups separate from your laptop or tablet.
- Password security: Secure devices with unique and secure passwords. Although biometric locks are convenient, they are considered less secure than strong passwords. Two-factor authentication can provide an additional layer of security.
- Know your rights
  - You are not required to share your password with CBP, but refusal may lead to device seizure (regardless of citizenship) and denial of entry for foreign nationals.
  - US citizens can refuse to answer questions beyond identify and travel details. Lawful permanent residents (green card holders) cannot be denied entry but may face

additional scrutiny and delay. Visa holders may be denied entry if they refuse to answer questions.

- Document the search: Write down details of the search including the names and badge numbers of CBP agents and the questions they ask. If your interview was recorded, ask for a copy of the transcript.
- 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. Consider travelling with a temporary phone and then transferring your SIM card or getting a new number at your destination.
- Encrypt your devices: Enable full-disk encryption on all your devices for added security. Use strong passphrases instead of simple passwords.
- 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.
- 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.
- 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.

Interacting with CBP Agents

- Be honest: Always tell the truth. Never lie to CBP officers.
- Stay calm: Do not argue or interfere with an inspection.
- Acknowledge CBP 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.