porterwright

Electronic Device Searches at U.S. Ports of Entry

U.S. CUSTOMS OFFICERS' AUTHORITY

- Customs officers have 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.
- Searches can occur without warrants at any U.S. ports of entry and CBP preclearance locations abroad, such as Dublin or Toronto.

TYPES OF SEARCHES

- A ***basic*** search is a manual search of an electronic device that can be done without suspicion and generally involves an officer reviewing the contents of the device without the assistance of any external equipment.
- An ***advanced*** search is 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. Officers 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.

KNOW YOUR RIGHTS

- You are not required to share your passwords, but refusal may result in consequences, explained below.
- **U.S. citizens** cannot be denied entry for refusing to provide access to their devices, but this may cause delays. Officers must let you enter the country; however, devices may be seized.
- **Lawful permanent residents (LPR)** who have previously been admitted and maintained status cannot be denied entry, but they may face additional scrutiny. Devices may be subject to seizure. LPR status may not be revoked without a hearing before an immigration judge.
- **Visa holders and temporary visitors** can be denied entry for refusing to provide access to their devices. Boarding may be denied at preclearance locations.

BEFORE YOU TRAVEL

- Consider traveling with devices free of sensitive data or apps that collect and store sensitive data.
- Consider leaving your usual phone at home and obtaining a temporary electronic device.
- Backup important files securely in the cloud or an external drive, separate from your laptop.
- Clear caches and cookies.
- Encrypt your devices for added security and secure devices with unique, complex passwords. Enabling two-factor authentication can provide an additional layer of security.
- Power down devices to help protect against potential remote access.
- Sign out of sensitive apps, disable automatic logins, and consider removing apps that store personal data.

IF YOUR DEVICE IS SEARCHED

- If you have privileged or sensitive material on your device, let officers know before they begin any search. Officers must follow certain procedures when privileged or other sensitive material is present.
- Officers may only examine information on the device at the time admission is sought and they cannot access information stored remotely (*aka* in the cloud). Searches are conducted while phones are in "airplane" mode.
- Write down details of the search, including questions asked and the names and badge numbers of officers.
- Inspect devices upon return by performing scans for any unauthorized software or changes.

HOW TO HANDLE INTERACTIONS WITH CUSTOMS OFFICERS

- Do not lie to Customs officers as lying can be a crime.
- Do not argue or interfere with an inspection.
- Understand that Customs officers have the authority to physically inspect electronic devices, but they cannot demand passwords. Refusing access to devices may result in consequences such as device seizure or denial of entry.

If you have questions about traveling to the United States, please contact any member of Porter Wright's Immigration Practice Group. This flyer is intended for general information purposes only and is not intended to be and should not be taken as legal advice.