CBP electronic device searches: What you need to know

As the U.S. government heightens its focus on national security, international travelers—especially visa holders and lawful permanent residents—are experiencing increased scrutiny at ports of entry.

U.S. Customs and Border Protection has broad legal authority to inspect and search electronic devices — including phones, laptops, tablets, USB drives, and external hard drives – at the border. These searches **do not require a warrant, probable cause, or even individualized suspicion**, and can be conducted as part of routine screening at any U.S. port of entry. CBP's authority extends to both incoming and outgoing travelers at any U.S. port of entry.

Here's a summary of what to expect at the border, your rights and responsibilities, and how to prepare.

Recent Executive Order: Heightened national security screening

On January 20, the White House issued Executive Order 14161: Protecting the United States From Foreign Terrorists and Other National Security and Public Safety Threats. This Executive Order directs federal agencies, including CBP and U.S. Citizenship and Immigration Services, to implement more rigorous screening procedures for individuals seeking entry into the United States.

Key implications for travelers include the following:

- Expanded data collection. The E.O. authorizes enhanced vetting measures and broader analysis of personal data, including social media activity and electronic records.
- More detailed questioning. Travelers may face additional scrutiny related to travel purpose, background, or affiliations.
- Longer processing times. Enhanced screening could result in delays at ports of entry.

Travelers should assume that both device content and online presence may be reviewed during inspection. Accuracy, consistency, and preparedness are essential.

CONSTANGY
Brooks Smith & Prophete

CBP electronic device searches: What you need to know

CBP device searches

CBP categorizes searches into two types:

No. 1: Basic search

- Officers may ask you to unlock your device and may manually examine its contents.
- Officers may browse through your photos, documents, contacts, call logs, emails, messages, downloaded apps, and browsing history.
- Officers cannot access cloud content unless it's already downloaded onto the device or auto-synced.
- You may be asked to put the device in airplane mode to prevent cloud-based data retrieval.

No. 2: Advanced search

- If flagged for further scrutiny, CBP may connect your device to a specialized forensic tool to copy, review, and analyze data.
- This could include hidden files or deleted content.
- CBP may retain the device temporarily (typically for no more than five days, though extensions are possible) for off-site analysis.

Social media scrutiny

In addition to CBP's authority to search devices, U.S. immigration agencies are expanding efforts to review the **digital footprints** of applicants and travelers. A recent notice proposes that the USCIS begin collecting **social media identifiers** from individuals applying for immigration benefits—including green cards, naturalization, asylum, and refugee status. This proposed rule reflects a growing trend toward incorporating social media review into vetting and background checks.

Travelers and visa applicants should consider doing the following:

- Review your profiles. Ensure your personal, employment, and location details match your immigration records.
- Adjust your privacy settings. Limit public access to sensitive content, while maintaining a professional presence.
- Be thoughtful about online posts and interactions. Avoid creating content that could be interpreted as inconsistent with your immigration status or entry purpose.
- Delete inactive or outdated accounts. Especially those that may contain conflicting personal details or old user names.

CBP electronic device searches: What you need to know

If you refuse to provide access

- U.S. citizens cannot be denied entry for refusing to unlock a device. However, non-citizens—including visa holders and lawful permanent residents—can be refused admission or face delays.
- It is important to note, in some cases, that CBP may seize the device, escalate questioning, or refer the case to other agencies.

Know the limits of your legal recourse

CBP's border search policies—including those on electronic devices—are governed by internal directives and longstanding federal law. These policies are designed to guide CBP operations but do **not** create or confer any personal rights, privileges, or legal remedies for travelers. In other words, travelers generally cannot sue CBP for following these policies unless a separate legal violation can be shown.

Traveling with electronics

To protect your privacy and reduce the risk of delays or data exposure, you should do the following:

Before you travel:

- Back up your device, and travel with minimal data.
- Log out of social media and email apps; disable biometric access (for example, Face ID, fingerprint).
- Consider using guest profiles or temporary "travel devices."
- Turn off cloud syncing, or remove apps that store sensitive information (for example, Slack, Dropbox, Signal).
- Encrypt your device, and use strong alphanumeric passwords.
- Consider storing critical work files or privileged content in secure cloud storage (and sign out of those services).

During travel:

- Cooperate respectfully if asked to unlock a device, but avoid volunteering access to apps or platforms.
- If detained or questioned extensively, ask to speak with legal counsel or your company's HR contact.

After re-entry:

- Monitor for signs of data access or tampering if your device was taken or searched.
- Consider changing passwords and enabling multi-factor authentication on sensitive accounts.
- Notify your legal or compliance team if any privileged, confidential, or regulated data may have been accessed.

Additional tips

- Be prepared to explain your travel purpose, employer, and visa status clearly and concisely.
- Ensure device data does not conflict with your stated purpose of entry.
- Avoid saving politically sensitive material or participating in online discussions that could be misinterpreted.

Filing a complaint

If you believe your device was mishandled or your rights were violated during a CBP search, you can file a redress request through the **Department of Homeland Security Traveler Redress Inquiry Program**, known as "TRIP" for short. TRIP is a formal avenue for travelers to inquire about or resolve issues related to CBP inspections, delays, or treatment at the border. Complaint or redress requests can be submitted here.

Unfortunately for international travelers—particularly visa holders and lawful permanent residents—electronic device searches are no longer rare exceptions but a routine part of CBP's screening authority. Travelers should assume that anything accessible on a personal device could be subject to review.

By anticipating potential scrutiny and following best practices, travelers can reduce complications at the border and better protect both their personal privacy and professional integrity.

Contact any member of Constangy's Immigration Team for further guidance.