Digital Privacy at the U.S. Border

At the U.S. border, such as ports of entry at land borders and international airports, U.S. Customs and Border Protection (CBP) asserts broad authority to search and seize the information on cell phones and other electronic devices. The government has more power at the border than other places, but the border is not a Constitution-free zone.

How can you prepare to cross the U.S. border?

Have a plan. It is important to have a plan before crossing the border. However, ONE SIZE DOES NOT FIT ALL! The most critical decision point is when you are pulled into secondary inspection and a CBP officer (or another federal agent) asks you to **unlock your electronic device or provide the passcode**. You must know ahead of time what you are going to do in that moment and how you are going to prepare your device(s) accordingly, depending on your individual circumstances.

Consider the risks. Consider your potential risks of crossing the U.S. border with electronic devices and how you might mitigate those risks. The primary risk is that you (and those you associate with) will suffer an **invasion of privacy** due to federal agents accessing and potentially copying the digital data on your device. You may also have your **device confiscated**. You may suffer a **loss of data**, due to your device being confiscated (if not backed up). You may be subject to **extended temporary detention and travel delay**. You may be subject to **extended questioning by and confrontations with** federal agents. You may be **denied entry** if you are not a U.S. citizen or Lawful Permanent Resident (green card holder). *These additional risks may be based on you refusing to grant access to your device or on information that border officers view on your device.*

Immigration status. The most important personal factor in deciding what to do is your immigration status. **U.S. citizens** have the most leverage to refuse to comply with a request to unlock an electronic device or provide the passcode because they must be let back into the country. However, they may be detained for several hours, subjected to additional questioning, and their devices may be confiscated for days, weeks, or months. **Lawful Permanent Residents (green card holders)** generally also must be let back into the country like U.S. citizens. However, as of 2025, the administration has displayed a willingness to challenge green card status, so these travelers should take this into consideration. For all **other non-citizens** (traveling on a visa or via the visa waiver program), refusal to comply may result in being denied entry.

Minimize the data you carry across the border.

- **Factory-reset your device**, or leave your primary device at home and travel with a **temporary device**, such as a "burner" phone or an internet-based laptop. However, be aware that these might raise suspicion and lead to additional questioning, and cheaper and older devices are generally more vulnerable to forensic search.
- **Delete sensitive data and apps** from your device. Do not forget to empty the trashcan and check for "recently deleted" folders in photos, browsers, and apps. However, be aware that even after removing an app, some data from it may be left over on the device.
- **Transfer data to cloud storage**, if you will have internet access to retrieve it later.

Protect what data you carry across the border.

- **Backup** your data before traveling.
- Enable full-disk **encryption**, not just a screen lock.
- Use **strong passcodes** (4-5 random words). See *https://eff.org/dice*.
- **Disable** biometric unlocks (face/thumb).
- **Power down** your devices.

EFF

Basic rules:

- Stay calm and respectful during secondary inspection.
- Do not lie to border officers or try to hide data on your device.
- Do not physically interfere with border officers.
- If you encounter any problems, document the names, badge numbers, and agencies of the officers you interact with at the border.
- Request a property receipt (Form 6051D) if your device is confiscated.

What does CBP's policy say?

- CBP's currently operative policy from 2018 provides that CBP officers may conduct **"basic" (manual) searches** of electronic devices without any individualized suspicion of wrongdoing by the traveler, and **"advanced" (forensic) searches** with "reasonable suspicion of activity in violation of the laws enforced or administered by CBP" or when "there is a national security concern."
- **CBP officers may NOT search live cloud content via a device**—they may only search information that is "resident" on a device. Thus, they must put a device in airplane mode or otherwise disconnect it from the internet. However, be aware that they may be able to view **cached content** and may have **separately viewed public social media content**.
- Information that is protected by **attorney-client privilege or is attorney work product** must be segregated from other data by a Filter Team.
- CBP officers may **confiscate a device indefinitely** if the device is protected by a passcode or encryption and they need more time to make a "determination as to its admissibility, exclusion, or other disposition."

How have federal courts applied the Fourth Amendment of the U.S. Constitution?

Default rule. The Fourth Amendment protects individuals from "unreasonable" searches and seizures by the government. It requires that the government generally obtain a warrant based on probable cause from a judge—that is, based on preliminary evidence that there is a fair probability that the thing or place to be searched or seized will uncover further evidence of a crime.

Border search exception. The U.S. Supreme Court and federal appellate courts have created more relaxed rules at the border. This is because the primary purpose of searching luggage, vehicles, or persons is customs enforcement (i.e., collecting duties and interdicting contraband), rather than general law enforcement. Thus, most border searches (such as "routine" luggage searches) do not require a warrant or any individualized suspicion of wrongdoing, while more intrusive "non-routine" searches (such as strip searches) require reasonable suspicion.

Device searches. The U.S. Supreme Court has not ruled on device searches at the border, thus different constitutional rules apply depending on where you enter the country. While most federal courts have granted deference to the government, two appellate courts have limited CBP's authority due to the significant privacy interests that travelers have in their digital data. The Ninth Circuit held that a *warrant* is required for cell phone searches if border officers are interested in **data other than digital contraband**. The Fourth Circuit held that a *warrant* is required for forensic searches of electronic devices at the border in furtherance of **domestic criminal investigations**.

Want more information?

- Read our more detailed **travel guides, CBP's device search policy, and all of EFF's border-related work**: *https://www.eff.org/border*
- Read EFF's **Surveillance Self-Defense** technical guide: *https://ssd.eff.org*

The Electronic Frontier Foundation is the leading nonprofit defending digital privacy, free speech, and innovation. https://eff.org