Crossing the U.S. border? Border agents may demand your digital data. Here are some things to keep in mind.

Consider your individual risk assessment factors. Your immigration status, travel history, the sensitivity of your data, and other factors may influence your choices.

**Before your trip:**
- **Reduce the data you carry.** Consider using temporary devices, deleting data from your regular devices, or shifting data to the cloud.
- **Encrypt.** Use strong full-disk encryption, not just weak screen-lock passwords.
- **Password.** Use software to make them long, unpredictable, and memorable.
- **Backup.** In case agents seize your devices.
- **Power down.** Do it before arriving at the border to block high-tech attacks.
- **Fingerprint locks.** They are weaker than passwords, so don’t rely on them.
- **Apps and browsers.** Agents use them to get cached cloud content. Consider logging out, removing saved login credentials, and clearing cloud content.

**At the border:**
- If you refuse, agents may seize your device.
- If you comply, agents may scrutinize and copy your sensitive data.
- If you are a U.S. citizen, agents must let you enter the country. If you are a lawful permanent resident, agents may seize your temporary travel documents.
- If you are a foreign visitor, agents might deny you entry.
- If you are a lawful permanent resident, agents might raise complicated questions about your continued status as a resident.

**But be aware:** Unusual precautions may make border agents suspicious.

**After your trip:**
- **Contact EFF at borders@eff.org.**
- **Write down the details of what happened, including names of officers.**

**Want more information?**
- Read EFF’s longer border guide at [https://www.eff.org/border-search](https://www.eff.org/border-search)
- Read EFF’s general surveillance self-defense manual at [https://ssd.eff.org](https://ssd.eff.org)