

Your iPhone at the U.S. border

Access US

Our lives are extensively documented on phones, laptops, and on social media. Some of this information is very personal, and a lot of travelers may wish to keep this sensitive data private. However, each time you enter the United States, regardless of your status or documentation, Customs and Border Protection (CBP) determines your admissibility to the country, and part of this determination may include searching a traveler's electronic devices. With these types of searches becoming increasingly common, it has never been more important for individuals to know and understand their rights at the border.

The U.S. border is considered a legal gray zone. This means that certain rights and freedoms granted to individuals under the U.S. Constitution do not necessarily apply. For example, the Fourth Amendment protects persons from unreasonable search and seizure. This is a fundamental right that has been engrained in the fabric of U.S. society, but it does not apply at the border. A customs officer's subjective belief that someone has, or is, engaged in any wrongdoing is enough to justify inspection. Officers can search a traveler's physical luggage, digital devices, social media accounts, and email accounts without a warrant. They can even keep your electronic devices for further examination, which could include copying your data. These standards apply to all travelers regardless of your immigration status.

If you are stopped at the border and asked for your passwords or the PIN to access your device, be careful in deciding how to answer. Refusing to provide this information can have serious consequences. A foreign national could be denied entry into the U.S., a green card holder could find themselves standing before an immigration judge, and a U.S. citizen could end up spending several hours waiting in secondary inspection. Keep in mind, these are worst case scenarios, but situations like this do arise.

If you travel to the U.S. on business and have sensitive corporate or client information on your devices, care should be taken when crossing the border. This means erring on the side of caution. You may want to consider leaving any privileged or sensitive information behind, and start using a travel computer and/or cell phone when entering the U.S. If that is not an option, another way to protect sensitive data is to store it on the cloud. This is a useful strategy for shifting data online, so that it is not present on your electronic devices when you cross the border. CBP can search your phone, but it does not have the authority to look through any information you have stored on a cloud service without first obtaining a subpoena or warrant. While this subject is expected to develop further over the next few months, it is still best practice to travel to the U.S. with "clean" electronic devices.

Rosanna Berardi is the Managing Partner at Berardi Immigration Law, a business immigration law firm based in Buffalo, New York. She can be reached at 877.721.6100 or rberardi@usimmlawyer.com.