Border Searches of Your Electronic Devices — What Rights Do You Have?

Written by Emily Nash

March 23, 2017

The United States government has reported that border searches of electronic devices in the U.S. increased from 4,764 in 2015 to 23,877 in 2016. Because electronic devices have immense data storage capacity and can hold confidential information, trade secrets and data otherwise protected by attorney-client privilege, these searches have raised alarm for individuals, and the companies that employ them, when traveling. Adding social media and cloud storage into the mix, a few additional passwords from a device could unlock a multitude of data not even technically on the device itself.

The Trump Administration's new restriction on electronic devices may signal an increase in electronics searches at international ports of entry. On March 21, 2017, the Department of Homeland Security announced a new policy banning laptops, tablets, cameras, and other electronic devices bigger than cell phones from cabins in foreign airlines where the flight originated from the following airports: Cairo; Istanbul; Kuwait City; Doha, Qatar; Casablanca, Morocco; Amman, Jordan; Riyadh and Jeddah, Saudi Arabia; and Dubai and Abu Dhabi in United Arab Emirates. The carriers operating out of those airports have until Friday to comply. Devices stored in checked baggage are still subject to search by customs agents.

Although many details of the new policy remain unclear, we expect border officers will be even more likely to search the devices of travelers from these countries. Individuals planning to travel to the U.S. on flights governed by the new policy should expect at least routine electronics searches.

Here are key considerations for businesses and travelers to comply with travel policies and searches.

What Types of Searches Can Be Expected?

U.S. Customs and Border Protection (CBP) officers, Immigration and Customs Enforcement (ICE) officers and other federal customs agents have broad authority to conduct "routine" or "cursory" searches of your electronic devices without suspecting you of any criminal wrongdoing. At the border, like searches of a person's suitcase or even their body, an agent may conduct a search of an electronic device without any suspicion at all if the search is "routine."

Routine Searches

In general, a search of your electronic device will qualify as "routine" if the agent conducts the search in your presence over a relatively short amount of time using no more advanced technology to look through your data than his or her own hands, clicking or scrolling through your device the way an average user would.

Therefore, in a routine search, a CBP officer can physically inspect your electronic devices, which is no different from any other container when it comes to a physical search. A physical search of the device—even one removing the battery and looking through the devices cavities—will not require any level of suspicion.

Non-Routine Searches

Searches that are "non-routine" generally require "reasonable suspicion" of criminal wrongdoing to be constitutional. Reasonable suspicion requires a showing of "objective, articulable facts that justify the intrusion as to the particular person and place searched." Officers may consider facts including your behavior, your criminal history, your travel history and any inferences officers may draw using

their experiences. Although there is no one definition of what constitutes a "non-routine" search, this type of search may involve seizing and retaining electronic devices for days or weeks, copying the device's contents, and using technology to view encrypted and even deleted data on the device.

Password-Protected Devices

A CBP officer can also view the data on your device if you have a password. A routine search includes turning on the device, opening and viewing image files, text messages, and using a computer's search functions to seek out particular files. In other words, anything an average cell phone or laptop user might be able to do, without the assistance of an external software program aiding the search, is fair game. Even if the search takes a few hours while you wait at the airport, it will probably be considered routine.

However, if you have a password and you do not provide that password to the agent conducting the search, the routine search may not be able to proceed any further. If you refuse to provide your password, but the agents guess your password and search your device, the search may still be considered routine. Note, however, that there are some special risks associated with denying an agent your password.

Do I Have to Provide my Password to Officers?

You are not legally required to provide CBP with passwords to unlock your devices or files. If you have a complicated password and do not provide it to an officer, you limit the amount he or she may see when conducting a routine search. After all, CBP officers also face practical limitations, like time and staffing, that prevent them from conducting hours-long searches of every traveler's devices. Nevertheless, you might want to provide your password anyway. Personal attributes may affect your risk calculation here, but no matter what, refusing to provide a password is risky. At minimum, the officer may escalate the situation, asking you more questions, and holding on to the device for a period of several hours to attempt to bypass the password, causing you to miss a connecting flight, if nothing else. At the other end of the spectrum, non-citizens and non-permanent residents could be denied entry for refusing to cooperate.

Do I Always Need to Consent to a Search?

The most important thing to note is whether you choose to give your password or not, make it clear that you are **not consenting** to the search. If the government can show you consented to the search, they will not need to show any level of suspicion at any point. If you choose to provide your password, an explicit statement to the effect of "I do not consent to this search," is in your best interest. Additionally, it is suggested that if you are going to provide a password, that you attempt to do so by entering it yourself, rather than providing it to the CBP officer. No matter what you do, do not give the CBP officer a password you know to be false; lying to or obstructing an investigation by a CBP officer is a crime.

What Should I Do with Protected Information?

If your device contains information protected by attorney-client privilege or confidential trade secrets, you might try telling the officers that. According to CBP policy, materials that are privileged and/or confidential are subject to higher standards than general information. For example, legal materials require an officer to "seek advice" from CBP chief counsel who will coordinate with the U.S. Attorney's Office as appropriate. In addition, the policy only provides confidential business information must be protected from unauthorized disclosure. So, if agents are not suspicious of you, they may listen. The explanation also solidifies your expression of non-consent without providing any basis of suspicion against you.

What Happens if Officers Seize my Device?

If CBP or ICE seize and retain your devices you should write down what happened. You should make sure you get a receipt listing the items that were seized, including the date of confiscation and the officer responsible for the seizure. You should also solicit a statement as to when the items would be returned. Note that ICE policy provides searches of electronic devices are to be completed within 30 calendar days of the date of detention. If the items are not returned within this period, you should have legal counsel contact DHS, CBP, and ICE, requesting return of the devices and documentation of the chain of custody of the devices, any copies that were made, and whether the copies were destroyed.

Conclusion

In general, even though border agents have broad authority to conduct electronics searches, their authority is not limitless. The law is far

from settled in this arena, and it is likely to evolve in the next few months and years. All travelers should assess their own risks, including immigration status, travel history, and data stored on the device before they decide how to best to proceed. It is prudent these days to carry as few electronic devices as possible and to protect devices by using a good password, as that cannot be used against you in a "reasonable suspicion" determination. It is also risky to refuse to provide a password; it is much riskier for a non-citizen to do so. Lastly, all travelers should be civil and respectful toward the CBP as much as possible. This will work to your benefit.

If you feel your rights were violated during a search, you should write down all of the details you can remember from the encounter and call our office immediately.

RELATED INDUSTRIES

- Technology

RELATED PRACTICES

- Immigration
- Litigation
