

IMMIGRATION

CROSSING THE BORDER WITH ELECTRONICS—HELPFUL TIPS AND PITFALLS TO AVOID

by Elise S. Levasseur, Esq.

International travelers have been reporting that cell phones, computers, and other communication devices are being seized by Officers of the U.S. Customs and Border Protection ("USCBP") branch of the U.S. Department of Homeland Security ("USDHS"), sometimes for a relatively short time, and sometimes for a number of days or weeks. In fact, according to recent news reports by NBC News on March 13, 2017,¹ there has been a five-fold increase in the number of electronic device seizures at U.S. ports-of-entry both when arriving and when departing in 2016 over 2015, and that trend is expected to continue. At risk is discovery of sensitive and commercially protected company data, company emails, company photographs, company videos, personal emails and personal photographs and personal videos.

Seizure of electronic devices is not a new phenomenon—it started with the George W. Bush administration, and has grown in recent years because of domestic terrorism, but it may be that the USCBP feels somewhat emboldened by President Trump's most recent Executive Orders on immigration, in which he ordered USCBP Officers to more aggressively enforce U.S. immigration laws, including making more use of regulations involving expedited removal. USCBP Officers have also been asking for passwords to social networking sites such as Facebook.

The Fourth Amendment of the U.S. Constitution protects individuals from unreasonable searches and seizures, but USCBP has long held the opinion that it has broad powers that extend 100 miles from any external border in the U.S. which is the so-called "border exception." It is important to understand that two-thirds of Americans live within 100 miles of an external border, and includes residents of Detroit, New York City, Los Angeles, Boston, Houston, etc.

Under the "border exception," when an individual is seeking admission to the U.S., or departing the U.S., USCBP does not have to demonstrate that it suspects that the person who is possession of a particular device is involved in crime, however certain recent case law indicates that the more invasive the search, the more evidence that a crime may have been committed or is about to be committed is required. According to USCBP's last published policy on seizure of electronic devices which was in 2009, officers can seize an electronic device or company information from the device for a brief time not to exceed five days, although an Officers can ask a Supervisor for an extension of time.

Various organizations, including the American Civil Liberties Union ("ACLU") have argued that the 2009 USCBP policy needs to be updated given that it hasn't kept up with the changing electronic device technology landscape, and that electronic devices are essentially like your desk or home and should be extended the same protections under the Fourth amendment, even at a port-of-entry. Furthermore,

there are privacy issues which may be given paramount concern over the USCBP's need to determine whether a crime will be or has been committed by seizure of electronic devices including: company trade secrets, attorney-client privileged information, doctor-patient confidentiality, health information, financial records, etc.

Until some of these issues are resolved, and they may never be completely resolved, it is a good idea to take some precautions when crossing the border with electronic devices. Various electronic device advocacy groups recommend certain practices, but clients are welladvised to work with qualified IT security specialists to assist them in ensuring that company data is secure when crossing into or out of a U.S. border. The recommendations are as follows:

- Where it is possible, don't take certain electronic devices with you when crossing the border;
- Consider carrying a mobile phone only used for foreign travel (although understand this may raise some concerns on the part of USCBP who may believe that the traveler is hiding something);
- Consider taking a special laptop that only contains minimum information, if possible;
- Consider taking a blank device and download data later, if possible;
- Be sure to back-up data in the event that the USCBP seizes a device;
- Consider using or transferring data to cloud services to store data;
- Never lie to officers of the USCBP. The consequences may be a lifetime bar against travel to the U.S. for making fraudulent statements to USCBP;
- Don't refuse to give USCBP a password to devices or social network sites, particularly if you are a foreign visitor or guest worker or Lawful Permanent Resident ("LPR") or you may find yourself refused admission after a lengthy delay;
- Consider deleting content or moving data to a cloud service but understand that deleted information or moving information to a cloud services may still be obtained by USCBP as USCBP has everincreasing technical ability to retrieve deleted or transferred data;
- Consider encrypting some of your data but understand that the USCBP's tools for uncovering encrypted data and/or passwords have improved significantly over the past few years;
- Always be considerate and polite to USCBP officers, especially if you are a Lawful Permanent Resident or green card holder and especially if you are a foreign visitor or guest worker;





- Understand that being rude to an officer or failing to cooperate even if you are a U.S. citizen can result in lengthy detention or delays in boarding flights or getting to meetings. USCBP knows full well that a delay is not something that you want and they may threaten it to get you to cooperate;
- If you are a U.S. citizen, (this is not recommended for LPR or foreign visitors and guest workers), consider asking the officer to reconsider the request, arguing that the device is not your property but the employer's property, or arguing attorney-client privilege, doctor-patient confidentiality, medical history, etc.;
- An LPR may not want to assert that the data is covered under various privileges because USCBP can challenge the LPR on how long he or she has been outside of the U.S. and for how long, to argue abandonment of status. Nonimmigrants, that is visitors, guest workers etc. can be refused admission and in some circumstances expeditiously removed;
- Do not obstruct the officer's search by refusing to provide the officer with a password or with refusing to give information related to the device or the device itself;
- Always get the officer's name, and other identifying information if there has been a seizure of a device, or if there has been an especially unpleasant encounter during which you believe your rights have been abused;
- Get a receipt for the seized item;
- If your rights have been abused, then consider filing a redress claim with the USCBP by going to <u>https://www.dhs.gov/dhs-trip;</u>
- Finally, it is important to understand that you are not afforded the right to counsel during either primary or secondary inspection at a U.S. port-of-entry, although depending on the severity of the circumstances, you can ask to speak with an attorney and carry with you an attorney's telephone number. This may result in the USCBP officer being less aggressive with you, but remember only to do this if the level of inquiry becomes excessive.

¹ America Citizens: U.S. Border Agents Can Search Your Cellphone, <u>http://nbcnews.com/news/us-news/american-citizens-u-s-border-agents-can-search-your-cellphone</u>, 3/13/2017

This client alert is published by Dickinson Wright PLLC to inform our clients and friends of important developments in the field of immigration. The content is informational only and does not constitute legal or professional advice. We encourage you to consult a Dickinson Wright attorney if you have specific questions or concerns relating to any of the topics covered here.

DW Immigration: Global Mobility with a Personal Touch!

FOR MORE INFORMATION CONTACT:



Elise S. Levasseur is a Member in Dickinson Wright's Troy office. She can be reached at 248.433.7520 or elevasseur@ dickinsonwright.com.



Christian S. Allen is Of Counsel in Dickinson Wright's Troy office. He can be reached at 248.433.7299 or callen@ dickinsonwright.com.



Lisa D. Duran is a Member in Dickinson Wright's Phoenix office. She can be reached at 602.285.5032 or Iduran@ dickinsonwright.com.



Suzanne K. Sukkar is Of Counsel in Dickinson Wright's Ann Arbor office. She can be reached at 734.623.1694 or ssukkar@dickinsonwright.com.



Kevin J. Weber is a Partner in Dickinson Wright's Toronto office. He can be reached at 416.367.0899 or kweber@ dickinsonwright.com.

