Secure Computing Abroad: Evolving Law Firm Policies

by Sharon D. Nelson, Esq. and John W. Simek

© 2017 Sensei Enterprises, Inc.

Traveling abroad? Worried about pickpockets? We have far bigger worries these days. If you travel abroad, you also have to worry about foreign governments – and our own – which may be interested in our data. Lawyers are not only not exempt from that interest – they are magnets. And when *The New York Times* published an article early this year about safeguarding data when crossing the border, we knew we were seeing a new hot cybersecurity topic – one that has primarily been considered at very large firms, until all the recent stories caught fire in the news. This article will focus on the dangers presented by our own government (the current runaway headline), but the advice is generally applicable to the risks presented by foreign governments, risks which may increase as there seems to be a worldwide ratcheting up of device seizure and examination at borders.

Three U.S. Border Incidents

There have been many, many border incidents, but here are three that caught our attention. A U.S.-born NASA scientist, Sidd Bikkannavar, returned to the U.S. in January of 2017. A seasoned international traveler, he flew back from Santiago, Chile to the George Bush Intercontinental Airport in Houston, Texas on Monday, January 30th, just over a week into the Trump administration.

Bikkannavar says he was detained by U.S. Customs and Border Patrol (CBP) and pressured to give the CBP agents his phone and access PIN. Since the phone was issued by NASA, it may have contained sensitive material that wasn't supposed to be shared. A Customs officer presented Bikkannavar with a document titled "Inspection of Electronic Devices" – which mentioned detention and seizure - and explained that CBP had authority to search his phone.

Bikkannavar was not allowed to leave until he gave CBP his PIN. Ultimately, feeling pressured, he agreed to hand over the phone and PIN. The officer left with the device and didn't return for another 30 minutes. The phone was returned to Bikkannavar, though he's not sure what happened during the time it was in the officer's possession. When it was returned, he immediately turned it off because he knew he had to take it straight to the IT department at NASA's Jet Propulsion Laboratory (JPL). The cybersecurity team at JPL was not happy about the breach.

Haisam Elsharkawi, an American citizen, was about to travel from Los Angeles to Saudi Arabia in February of 2017 when he was stopped at the airport, questioned, handcuffed, questioned some more and then released without charges three hours after his flight had departed. He reported that officers from the United States Customs and Border Protection repeatedly pressured him to unlock his cellphone so that they could scroll through his contacts, photos, apps and social media accounts. He said they threatened to seize the phone if he did not comply.

Also a veteran international traveler, he was appalled but felt pressured to unlock his phone and a Homeland Security agent looked through it for about 15 minutes.

In October of 2016, border agents seized phones from a Canadian photojournalist. He refused to unlock the phones, citing his obligation to protect his sources – he was blocked from entering the U.S.

As of March 13, 2017, NBC News had examined 25 cases in which American citizens said that CBP officials demanded that they hand over their phones and their passwords – or unlock them. In 23 of the 25 cases, these individuals were Muslim.

Keeping Private Data Private

Stories like these prompted *The New York Times* to investigate how to protect private data. As the paper states, U.S. citizens are not required to unlock their phones or share passwords with U.S. government officials. However, rules may vary depending on where you are traveling to and from. But being detained and intimidated is not an experience any traveler wants to go through.

So the *Times* recommended traveling with clean phones (so-called "burner" phones are often available at airports, as are phones you can rent) and clean tablets or laptops. It is recommended that you disable fingerprint readers because, in the U.S., law enforcement agencies can use warrants to compel you to unlock your phone with your fingerprint. We would go further and advise disabling all biometrics used to get into your phone, such as iris scans and facial recognition.

If you tell an official that you will not give up your password, the official may not be happy - to put it mildly. Better to use a password manager and tell the agent that you don't remember your one very long master password. And to avoid complications, don't have your password management software loaded on your devices. It is best to store the password vault (encrypted of course) in a cloud service like Dropbox and get access to it when you reach your destination.

If you are asked for passwords to your social media accounts or your e-mail, you can protect yourself by having two-factor authentication enabled – assuming that you have left your phone at home. Since the text code will be sent to that phone, officials will be unable to get into your accounts even with your password. You could leave your phone with someone you trust and get those codes that way but the general advice is to forego the use of social media while abroad.

When dealing with e-mail, do not install and configure any e-mail client on your laptop or cell phone. You don't want to have any e-mail on your devices. You should use some sort of remote access solution (e.g. Citrix, LogMeIn, etc.) to access your e-mail. Even using a browser could leave remnants of confidential information on your device.

Any device you use while abroad should be encrypted. The best way to ensure that your data remains secure is to back up your data to a cloud service and then wipe all of your devices before you return home. Once home, you can restore your data from the backup.

No matter what device you use abroad, assume that all electronic communication is subject to interception. This means you should always be using a secure encrypted connection. Make sure you have a properly configured VPN available and know how to use it.

The Authority of U.S. Customs and Border Protection Agents

Not only were we almost completely ignorant about the authority of CBP agents, it turns out that most lawyers have little knowledge of how expansive CBP authority really is. CPB officers have search power extending 100 air miles inland from any external boundary of the U.S. They can stop and question people at fixed checkpoints dozens of miles from U.S. borders. They can also pull over motorists whom they suspect of a crime as part of roving border patrol operations.

You might say - But doesn't the Fourth Amendment protect us from "unreasonable searches and seizures?" Yes – however, those protections are lessened when entering the country at international terminals at airports, other ports of entry and any location within 100 air miles of a U.S. boundary.

According to federal statutes, regulations and court decisions, CBP officers have the power to inspect, without a warrant, any person trying to gain entry into the country – and their belongings. The CBP's authority extends to examining computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players, and any other electronic or digital devices. That cuts a wide swath.

Current CBP policy dictates that officials should search electronic devices with a supervisor in the room when feasible and also in the presence of the person being questioned "unless there are national security, law enforcement or other operational considerations" that take priority. We already know that this language has been invoked to examine devices outside the presence of the person being questioned. CBP says it can conduct these searches "with or without" specific suspicion that the person possessing the items is involved in a crime.

With the approval of a supervisor, CBP officers can seize an electronic device – or a copy of the information on the device – "for a brief, reasonable period of time to perform a thorough border search." Typically, such seizures should be no more than five days (which seems a lot to us), but officers can apply for extensions in up to one-week increments. If the review of the device and its contents doesn't manifest probable cause for seizing it, CBP says it will destroy the copied information and return the device to the owner.

What if you are a lawyer? CBP has recognized that lawyers have an attorney-client privilege, but all this seems to mean is that agents have to get approval from an agency attorney before proceeding with the search. Not terribly comforting – and we suspect this is the reason why we have seen so many firms begin specifically to address the potential problems of re-entering the U.S.

What Have the Courts Said?

Unfortunately, the Supreme Court has not directly ruled on whether the CBP can search electronic devices without any specific suspicion that the owner might have committed a crime. In 2013, a decision for the U.S. Court of Appeals for the Ninth Circuit (http://cdn.ca9.uscourts.gov/datastore/opinions/2013/03/08/09-10139.pdf) affirmed that a cursory search of a laptop – for instance, having an owner turn on his/her devices and examining their contents – does not require any specific suspicions about the traveler. The court raised the bar for a "forensic

examination" of the devices such as using "computer software to analyze a hard drive." For these more comprehensive and intrusive searches, including password-protected information and other private data, officials must have a "reasonable suspicion" of criminal activity. That court decision applies only to the nine Western states in the Ninth Circuit.

We like this quote from the court's decision: ""Laptop computers, iPads and the like are simultaneously offices and personal diaries. They contain the most intimate details of our lives . . . It is little comfort to assume that the government — for now — does not have the time or resources to seize and search the millions of devices that accompany the millions of travelers who cross our borders. It is the potential unfettered dragnet effect that is troublesome."

During the 2016 fiscal year, CBP officials conducted 23,877 electronic media searches, five times as many as in 2015. That's a striking escalation.

What Law Firms Are Doing

As part of our research for this article, we were given access to one law firm's security precautions when traveling abroad. They included the following guidelines:

- Use one of the firm's "clean" loaner laptops, wiping the laptop before returning home
- Store all documents on the firm's network – store nothing on the laptop
- Use a burner phone (not a smart phone) for calls and texting.
- Access the firm's network via Citrix for e-mail and documents from the laptop - do not access the network from the phone.
- Do not use Bluetooth.
- Lock the laptop in the hotel room safe or in locked luggage.
- Make sure microphones and cameras are turned off.
- Change your network password before leaving the U.S., change it again once you return, after you have turned in your loaner laptop.

We have boiled the essential instructions down – as you can imagine, the instructions are far more detailed. A guiding principle is that authorities cannot search what you don't have. For those who want to chance it and have their device/data with them, make sure the device is encrypted and that it is powered down before going through Customs.

Several experts have published arcane methods of protecting your data, but we have not included them as being beyond the ken of most attorneys. And none of them will protect you from actually facing an angry CBP (or foreign) agent telling them that you really don't have any way to get to your data. We much prefer the "they can't search what you don't have" way of thinking.

In March of 2017, The Electronic Frontier Foundation published a fairly lengthy guide called "*Digital Privacy at the U.S. Border: Protecting the Data on Your Devices and in the Cloud*" which is worth reading and may be found at https://www.eff.org/wp/digital-privacy-us-border-2017.

Conclusion

In an article, it is impossible to examine every possible precaution that lawyers might use to protect client data while abroad. And though we've focused on the U.S. border because of current events, we have spent years watching videos of the Chinese spies accompanying maids to hotel rooms and inserting a flash drive in a businessman's computer. And we've heard stories from our large law firm friends of laptops coming back from abroad with "a little something extra" – that transmits data back "home". If you are a mid-to-large firm lawyer, your firm probably has very competent IT/cybersecurity help to assist you – don't be afraid to ask questions! And if you are a solo or small firm lawyer, make sure you engage someone who has both technical and security certifications to help you make sure you have the necessary security precautions in place.

The authors would like to thank their friend, journalist Ben Kerschberg, for his kind assistance in researching some aspects of this article.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, cybersecurity and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com