Focus INTERNATIONAL TRADE

There are no digital secrets at the border

Think twice before travelling with sensitive business data on electronic devices

Rosanna Berardi

AURIELAKI / ISTOCKPHOTO.COM

Each day, hundreds of foreign nationals travel to the United States for business meetings. Most business travellers carry a laptop and smartphone that contains confidential business information. This information may include e-mails from lawyers, proprietary data and trade secrets.

Imagine this: upon presenting your passport to Customs and Border Protection, you are unexpectedly pulled to the side and brought into secondary inspection. The officer asks for your cell phone and the password to access its content. Not knowing what else to do, you nervously hand the officer your cell phone and give him the password. The officer takes your phone and goes into the next room for more than an hour while you anxiously wait for his return.

If you frequently travel to the U.S. for work, it is not out of the realm of possibility that this could happen to you. Electronic media searches at the border are becoming a growing trend. In fiscal year 2016, 390 million people entered the U.S. and 23,877 electronic media searches were conducted at the border, compared to only 4,764 electronic media searches in fiscal year 2015.

In the wake of President Trump's recent executive orders pertaining to immigration, many travellers are confused and nervous about entering the United States as well as the scope of CBP's search authority. U.S. citizens, green card holders and visa holders alike can all be stopped at the border or taken into secondary inspection. This could be a random search or the officer may need more information about you or your immigrant status to decide whether they should allow you into the country. Essentially, each time you enter the United States, regardless of your status or your documentation, the officer is determining your admissibility.

The U.S. border is considered a legal gray zone in terms of given rights. The Fourth Amendment of the U.S. Constitution, which protects against unreasonable search and seizure, does not apply at the border. Border officers have the right to search travellers' physical luggage without a warrant and this interpretation has been expanded to include digital devices. While the Ninth Circuit Court of Appeals ruled in 2013 that agents need to have reasonable suspicion of wrongdoing to perform a full forensic search, the court stopped short of requiring officers to obtain a search warrant beforehand.

> **Extreme caution should be taken if you are determining whether to decline to provide your passwords or PIN. If you are a foreign national and are perceived as not being co-operative by withholding your information, you could be denied entry into the United States.**
>
> **Rosanna Berardi**
> Berardi Immigration Law

So, what does this mean for your "privileged" corporate data? Under current law, an officer can look through a cell phone or other electronic device in a cursory search for any reason. Rules like HIPAA (Health Insurance Portability and Accountability Act) and the attorney-client privilege do not apply at the border. This pertains to all travelers, including U.S. citizens, green card holders and visa holders.

The same rules apply to e-mail and social media. Even if you are a U.S. citizen, CBP officers can ask you for your e-mail login and password and social media profiles and log-ins. Additionally, while still in the preliminary discussion level, Trump administration officials are considering requiring foreign visitors to the U.S. to disclose the websites and social media platforms they frequent, as well as their log-in information. This discussion comes as an attempt to spot and deny entry to individuals who have ties to terrorist groups.

Extreme caution should be taken if you are determining whether to decline to provide your passwords or PIN. If you are a foreign national and are perceived as not being co-operative by withholding your information, you could be denied entry into the United States. If you are a green card holder, you may request a hearing before an immigration judge. You would likely be allowed into the country to await that hearing. If you are a U.S. citizen, you cannot be denied entry into the U.S., but you can be delayed. This could mean spending several hours in secondary inspection, but ultimately, they must let you back into the country.

Business travellers to the U.S. should be cautious about travelling with their laptops and cell phones. It is sound advice to "scrub" your devices and leave any "privileged" or "sensitive" information in Canada. We recommend that travellers, regardless of their immigration status, save their sensitive data at an off-site location. While this area is expected to evolve in the coming months, it is best to travel to the U.S. with "clean" electronic devices.

Rosanna Berardi is a business immigration lawyer and managing partner at Berardi Immigration Law, based in Buffalo, N.Y. For further information please call 877.721.6100 or email rberardi@uslmmlawyer.com.

We want to hear from you!
Send us your verdict:
comments@lawyersweekly.ca

Ratification: Most of the agreement could be applied on a provisional basis

Continued from page 15

Finally, it is important to note that not all of the CETA will take effect this spring. It is, in the parlance of the EU, a "mixed" agreement, within the competency of both the EU itself and its member states so it will not formally enter into force until it has been ratified by each of those 28 states (or 27 post-Brexit). Because that might not happen for several more years at least, Canada and the EU provided in the text that most of the agreement, the parts that are not exclusively within the competence of the member states, could be applied on a provisional basis.

That is what will happen this spring, once both parties have enacted the necessary implementing measures. In Canada, this is being accomplished through Bill C-30, now in the Senate, and by some changes to provincial and territorial procurement regimes.

Nearly all of the CETA will be provisionally applied, including the commitments already described. A notable omission will be investment protection commitments that were an important cause of the agreements prolonged gestation period. However, the practical consequences are limited because Canadian investors already have direct access to foreign investment protection agreements with seven of the more risky EU member states and may have indirect access to others depending on how their EU investments are structured.

Despite some shortcomings, the CETA will create real opportunities for Canadian businesses. Those opportunities can grow over time thanks to the institutional and substantive arrangements built into the agreement. With provisional application just a few months away, now is the time for companies to assess how to take advantage of what the CETA has to offer.

Matthew Kronby is a partner in the international trade and investment law group of Bennett Jones LLP. Before joining Bennett Jones he was the government of Canada's chief counsel in the CETA negotiations.