Does the Canada Border Services Agency Have the Authority to Search Your Electronic Devices?

Date: August 08, 2018

Original Newsletter(s) this article was published in: Blaneys on Immigration: August 2018

At the beginning of this year, I discussed the issue of border searches of electronic devices performed by United States Customs and Border Protection ("USCBP"). Of course, similar issues arise on the Canadian side of the border as well. For this reason, I will now discuss border searches of electronic devices performed by the Canada Border Services Agency ("CBSA").

Background

According to Subsection 99(1) of the *Customs Act*[1], CBSA officers have the authority to search goods being imported into Canada. In particular, Clause 99(1)(a) states that an officer may "examine any goods that have been imported and open or cause to be opened any package or container of imported goods and take samples of imported goods in reasonable amounts." This type of routine search does not require any reasonable suspicion on the part of the CBSA officer.

In addition, Subsection 139(1) of the *Immigration and Refugee Protection Act*[2] permits CBSA officers to search any person seeking to come into Canada, their luggage and personal effects, and the means of transportation that conveyed the person to Canada if the officer believes on reasonable grounds that the person:

a. Has not revealed their identity or has hidden on or about their person documents that are relevant to their admissibility; or

b. Has committed, or possesses documents that may be used in the commission of an offence relating to human trafficking or document fraud.

In *R.* v. *Simmons*[3], the Supreme Court of Canada ("SCC") recognized that international travelers have a reduced expectation of privacy when crossing the border. It also indicated that

there were three distinct levels of border searches (routine searches, strip searches, and cavity searches), each of which raised different constitutional issues. The more intrusive the search, the more reasonable justification is required.

Although the SCC has not directly addressed the constitutionality of suspicionless smartphone and laptop searches performed at the border, lower courts have found that such searches are permitted.[4] The term "goods" is defined in Subsection 2(1) of the *Customs Act* to include "conveyances, animals *and any document in any form*." These lower courts have found that computers, cell phones, and other electronic devices fall within the meaning of this term.

The courts have also concluded that routine border searches of smartphones and laptops in the border context do not require reasonable grounds. In *R.* v. *Sekhon*[5], the British Columbia Court of Appeal found that, as part of the normal course of the screening process, routine searches may be random and do not require grounds to search. In *R.* v. *Leask*[6], the Ontario Court of Justice concluded that border searches of a laptop computer are considered routine searches, which do not require reasonable grounds.

Of course, privacy advocates continue to argue that CBSA's authority to search electronic devices should not be exercised in the same manner as a briefcase or suitcase. This is because hand-carried electronic devices now have the capacity to store a very large amount of personal or business information. However, prior attempts to argue that electronic devices should be treated differently, in the context of border searches, have so far been unsuccessful.

CBSA Policy Guidance on Border Searches of Electronic Devices

Although the courts have not established any limits on the authority of CBSA to perform suspicionless searches of smartphones and computers at the border, CBSA's Operational Bulletin PRG-2015-31 ("OB PRG-2015-31") has purported to impose some limited restrictions on this authority. Although Operational Bulletins are theoretically binding on CBSA officers, they are not legally enforceable by third parties (i.e. travellers) in court.

Searches of Electronic Devices Not to Be Conducted as a Matter of Routine

According to OB PRG-2015-31, CBSA officers should conduct an examination of digital devices and media with as much respect for the traveller's privacy as possible, considering that these examinations are usually more personal in nature than baggage examinations. Such an examination must always be performed with a clear nexus to administering or enforcing CBSA-mandated program legislation that governs the cross-border movement of people and goods, plants and animals. CBSA officers shall not examine digital devices and media with the sole or primary purpose of looking for evidence of a criminal offence. They must also be able to explain their reasoning for examining the device.

Examinations of electronic devices pursuant to the *Customs Act* should not be conducted as a matter of routine. They should only be conducted if there is a "multiplicity of indicators" suggesting that evidence of contraventions may be found on the digital device or media. Where this occurs, or further to the discovery of undeclared/prohibited/falsely reported goods, officers

are authorized to conduct progressive examinations of digital devices and media for evidence of contraventions or to support allegations.

Initial examinations of digital devices and media should be cursory in nature and increase in intensity based on emerging indicators. CBSA officers must make notes describing the indicators that led to the progressive search of the digital device or media, what areas of the device or media were accessed during the search, and why.

In addition, examinations of electronic devices under the *Immigration and Refugee Protection Act* must be confined to identifying the person, finding documents relevant to admissibility or that may be used in the specified offences, or finding evidence of the specified offences. Where the identity or admissibility of a traveller is in question, CBSA officers are justified in performing examinations of digital devices and media to discover the traveller's true identity, evidence of false identities, or other documentary evidence pertaining to admissibility.

Searches of Data Stored in the Cloud

In *R.* v. *Gibson*[7], the Provincial Court of British Columbia held that the definition of "goods" included data stored in any electronic device (including cell-phones) that is in "actual possession of or in accompanying baggage of traveller at time they arrive at border and commence dealings with customs officers." However, it did not include data stored in the cloud or stored remotely on devices that were not in possession of the traveller.

Although *R.* v. *Gibson* is not necessarily binding outside of British Columbia, CBSA appears to have adopted the decision, which means that it should apply at all ports of entry, not only those located in the Province of British Columbia. OB PRG-2015-31 states the following:

Prior to examination of digital devices and media, and where possible, CBSA officers shall disable wireless and Internet connectivity (i.e. set to airplane mode) to limit the ability of the device to connect to remote hosts or services. This will reduce the possibility of triggering remote wiping software; *inadvertently accessing* the Internet or *other data stored externally*; or changing version numbers or dates.

Handling of Passcode Protected Devices

OB PRG-2015-31 states that, in instances where access to digital devices and media is password protected, officers are to request the password to access the device and record it, as well as any alternate passwords provided, in their notes. However, passwords are not to be sought to gain access to any type of account (including any social, professional, corporate, or user accounts), files, or information that might potentially be stored remotely. CBSA officers may only request and make note of passwords required to gain access to information or files if the information or file is known or suspected to exist within the digital device or media being examined.

OB PRG-2015-31 is silent regarding whether CBSA officers will charge a traveler with a criminal offence for refusing to provide his or her password. However, the *Customs Act* gives them the

authority to do so. According to Section 153.1, no person shall, physically or otherwise, do or attempt to do any of the following:

a. Interfere with or molest an officer doing anything that the officer is authorized to do under the Act; or

b. Hinder or prevent an officer from doing anything that the officer is authorized to do under the Act.

According to 160.1, every person who contravenes Section 153.1 is guilty of an offence and, in addition to any penalty otherwise provided, is liable on summary conviction to:

a. A fine of not less than $1,000 and not more than $25,000; or

b. Both a fine described in paragraph (a) and imprisonment for a term not exceeding twelve months.

Although CBSA officers appear to have the authority to impose criminal charges on an uncooperative traveler, it is more likely that one of more of the following will occur:

a. At the very least, a refusal to provide the password for a smartphone or laptop will significantly increase the CBSA officer's level of suspicion. This may prompt a more aggressive inspection and/or a more detailed examination of the electronic device.

b. Although Canadian citizens and permanent residents of Canada cannot not be denied entry to Canada, other foreign nationals could be refused admission for failing to establish that they are admissible.

c. CBSA could detain the electronic device for further examination. Under Section 101 of the *Customs Act*, goods that have been imported may be detained by a CBSA officer until he or she is satisfied that the goods have been dealt with in accordance with the Act (or any other Act of Parliament that prohibits, controls, or regulates the importation or exportation of goods). However, in *R.* v. *Gibson*, the Provincial Court of British Columbia found that detention of an electronic device for a full, forensic examination (i.e. copying data, utilizing password-cracking software, etc.) would require reasonable suspicion.

Conclusion

Despite the fact that an electronic device is actually very different from a suitcase, due the vast amounts of personal data that it may hold, Canadian lower court decisions do not currently recognize the distinction. The issue may eventually be addressed by the Supreme Court of Canada but, for the moment, CBSA officers appear to have the authority to perform suspicionless searches of smartphones and laptops in the context of a border inspection.

Although travellers may feel that such searches of their electronic devices are an unreasonable violation of their privacy rights, they need to be aware that refusing to provide their password can have serious consequences. Such travellers may wish to consider one of more of the following strategies:

a. Store any sensitive information in the cloud rather than storing it on the electronic device itself. CBSA's authority to search electronic devices theoretically should not extend to data stored remotely. Please note that some apps store a local copy of remotely-accessed data (for example, emails) on the device itself. If any data is resident on the device, it is fair game so care should be taken to ensure that this locally-saved data is removed from the device before travelling.

b. Use a complex, hard-to-guess password. Although refusing to provide password information to CBSA is not recommended, if the traveler ultimately chooses to do so, a hard-to-guess password will make it more difficult for CBSA to access their data, even if they perform a forensic examination of the device.

---

[1] R.S.C., 1985, c. 1 (2nd Supp.).

[2] S.C. 2001, c. 27.

[3] [1988] 2 S.C.R. 495.

[4] *R.* v *Buss*, 2014 BCPC 16; *R.* v. *Moroz*, 2012 ONSC 5642 (Sup. Ct.); *R.* v *Whittaker*, 2010 NBPC 32.

[5] 2009 BCCA 187, 67 C.R. (6th) 257.

[6] 2008 ONCJ 25.

[7] 2017 BCPC 237.