

CAUT Briefing Note

Supplement to 2005 CAUT Travel Advisory

The June 2005 CAUT Advisory on Travel to the United States considers traveler rights at land border entry points to the US as well as in preclearance zones at Canadian airports. The preclearance review is based on the 1999 *Preclearance Act*.

In October 2017, the Travel Advisory was revised in light of proposed changes in preclearance rules arising from the introduction of Bill C-23, a new version of the *Preclearance Act*. The Advisory also reviewed issues related to the search of electronic devices at border and preclearance zones.

This revised Briefing Note includes updates through July 2019.

Preclearance

In March 2015, Canada and the United States signed the *Agreement on Land, Rail, Marine, and Air Transport Preclearance*, which required both countries to implement new legislation. The United States Congress passed legislation in December 2016.

The Canadian legislation, the *Preclearance Act*, Bill C-23, was introduced in the House of Commons in June 2016. While Bill C-23 received Royal Assent on December 12, 2017, as of July 2019, the *Act* has not received the Cabinet approval necessary to bring it into force. In the meantime, the 1999 *Act* reviewed in the 2005 Travel Advisory remains in effect.

The debate around Bill C-23 focused on the enhanced powers under Part 1 accorded to United States Custom and Border Protection (CBP) officers in preclearance

zones located in Canada. These concerns may be the reason for the delay in bringing the 2017 *Preclearance Act* into force.

Other elements of the new *Act* include provisions for Canada Border Services Agency (CBSA) officers operating in preclearance zones that, pursuant to the Canada-US 2015 Agreement, may be set up by Canada at US locations. In the meantime, issues with respect to the powers granted to border agents to search electronic devices continue to arise at both the Canadian and American entry points.

Search of Electronic Devices

For CAUT members, reports that border officers' demands for access to electronic devices such as laptops, notepads and cell phones raise issues concerning the protection of research confidentiality and the exercise of academic freedom.

While the powers granted to border agents may not be new, they are being newly exercised.

Travelling to Canada

The Office of the Privacy Commissioner of Canada provides the following statement in respect to the inspections and searches of electronic devices at Canadian points of entry:

At border controls, Canada Border Services Agency (CBSA) officers have widespread powers to stop and search people, and examine their baggage and other possessions including devices such as laptops and smartphones. Under Canada's "Customs Act," these activities may be conducted without a warrant.

Canadian courts have generally recognized that people have reduced expectations of privacy at border points. In this context, privacy and other Charter rights continue to apply but are limited by state imperatives of national sovereignty, immigration control, taxation and public safety and security. To our knowledge, the Canadian courts have not yet ruled on whether a border officer can compel a person to turn over their password so that their electronic device may be searched at a border crossing.

While the law is unsettled, CBSA policy states that examinations of personal devices should not be conducted as a matter of routine; such searches may be conducted only if there are grounds or indications that “evidence of contraventions may be found on the digital device or media.”

If your laptop or mobile device is searched, it should be searched in line with this policy and you will likely be asked to provide your password. According to the policy, officers may only examine what is stored within a device, which includes, for example, photos, files, downloaded e-mails and other media. Officers are advised to disable wireless and internet connectivity, limiting access to any data stored external to the device, for instance, on social media or in a cloud. If you refuse to provide your password, your device may be held for further inspection.¹

The statement reflects the relevant CBSA directives and policies, but the powers of CBSA officers flow not just from the *Customs Act* but also from the *Immigration and Refugee Act*. Thus, in respect to searches of electronic devices, CBSA officers may rely on the *Customs Act* if the concerns relate to potential customs violations, or the *Immigration and Refugee Act* if the concerns relate to identity and/or threats to security.²

A refusal to provide a password to allow border officials to access an electronic device may result in the device

being held by CBSA, but not the arrest of the person failing to cooperate. It should be noted that the CBSA *Operational Bulletin* emphasizes that a request to search an electronic device and/or demand a password should be performed “with as much respect for the traveler’s privacy as possible, considering that these examinations are usually more personal in nature than baggage examinations.”³

Further, the power to examine an electronic device does not extend to accessing links to information not actually downloaded on the device. Indeed, CBSA officers are instructed to immediately put the device into “airplane” mode on initial access.

In August 2016, a Quebec resident was convicted and fined \$500 for obstructing border officials for refusing to give up his smartphone password on re-entry to Canada at the Halifax airport. The charges were brought under the *Customs Act* and CBSA concerns were evidently related to goods the individual may have been seeking to bring into Canada.⁴ As the defendant pled guilty, there was no trial, nor any ruling on the issue as to whether CBSA officers do indeed have the legal authority to require travelers to provide passwords to electronic devices such as cell phones.⁵

In April 2019, a lawyer’s phone and laptop were confiscated by a CBSA officer at Toronto’s Pearson Airport when he refused to provide passwords. The lawyer maintained that both devices contained confidential information protected by solicitor-client privilege. Although he was not detained, the devices were sent to a government facility which would try to crack his passwords and search his files.⁶

For academics, these claimed powers to examine the contents of a laptop, notebook or cell phone suggest that keeping research information or information gathered in

1. “Your privacy at airports and borders: Canadian Custom Searches,” *Public safety and law enforcement*, Office of the Privacy Commissioner of Canada, 2016. Accessed on-line at: <https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/your-privacy-at-airports-and-borders/>
2. “Operational Bulletin: PRG-2015-31: Examination of Digital Devices and Media at the Port of Entry” Canada Border Services Agency, 2015.
3. See “Actions required by CBSA officers” on page 2 of “Operational Bulletin: PRG-2015-31.”
4. Ruskin, Brett. “Alain Philippon pleads guilty over smartphone password border dispute,” *CBC News: Nova Scotia*, 2016.

- Accessed on-line at: <https://www.cbc.ca/news/canada/nova-scotia/alain-philippon-to-plead-guilty-cellphone-1.3721110>
5. Bailey, Sue. “Border phone search raises privacy, charter issues, say lawyers.” *CBCNews: Nova Scotia*. 2016. Accessed online at: <https://www.cbc.ca/news/canada/nova-scotia/alain-philippon-cbsa-border-cellphone-smartphone-search-1.3724264>
 6. Harris, Sophia. “Canada Border Services seizes lawyer’s phone, laptop for not sharing passwords”, *CBC News: Business*, 2019. Accessed on-line at <https://www.cbc.ca/news/business/cbsa-boarder-security-search-phone-travellers-openmedia-1.5119017>

the context of academic freedom on electronic devices may create a risk that such information will be reviewed at a Canadian port of entry or subject to examination after confiscation.

Travel to the United States

Issues with respect to travel to the US extend beyond inspection and search of electronic devices, given the recent Presidential Executive Orders and the apparent application of a heightened ethnic and religious screening process by CBP officers despite the injunctions against the implementation of those Orders.

Concerns about the privacy of confidential information on an electronic device when seeking entry to the US are bolstered by the apparently broader application of purported search powers by US Custom and Border Protection officers over that practiced by CBSA officers at the Canadian border.⁷ For example, CBP officers may ask for passwords not just to access the electronic device, but also to access external sites linked to the device such as social media or websites. The scope for privacy intrusion is thus even more extensive.⁸

The expansion of what the Americans call “warrantless searches” is the subject of litigation in US Courts. The focus in the US is not “customs search”, but security surveillance that has led to an increase in the number of device searches at entry into the United States. This has an impact on the privacy of not just the traveler, but the privacy of all those that can be identified through the contacts and communications on the devices.⁹

US residents may challenge these searches in domestic courts. That is less than a satisfactory option given the privacy breach has already occurred. However, there is really no effective legal way for a Canadian resident to challenge the actions of US border officers at a US point of entry.¹⁰ Failing to cooperate likely means you will be

turned away at the border —perhaps without the electronic device in question.

Conclusion

Travelers leaving or returning to Canada are increasingly vulnerable to border searches that may compromise research confidentiality and academic freedom. CAUT will continue to provide updates as developments occur. In the interim, it is recommended that academics carefully consider what information they have on their devices when crossing borders and take actions to protect sensitive information where necessary.

7. Greenberg, Andy. “A Guide to Getting Past Customs with your Digital Privacy Intact,” *Wired*, 2017,.. Accessed on-line at: <https://www.wired.com/2017/02/guide-getting-past-customs-digital-privacy-intact/>

8. Waddell, Kaveh. “Give Us Your Passwords,” *The Atlantic*, 2017. Accessed on-line at: <https://www.theatlantic.com/technology/archive/2017/02/give-us-your-passwords/516315/>

9. Noguiera, Daniela L. “Warrantless device searches at the border will threaten privacy in the US heartland”, *The Guardian*. July 18, 2019. Accessed on-line at:

<https://www.theguardian.com/commentisfree/2019/jul/18/us-border-warrantless-device-searches-cellphones-court-hearing>

10. There may be scope to challenge the exercise of such powers by CBP officers in a US preclearance zone such as a Canadian airport. The laws of Canada, including the Charter of Rights and Freedoms, continue to apply as this remains domestic territory, But again the choice may come down to agree to the search or be denied travel and any subsequent legal proceedings may not provide a meaningful remedy as the Court would not be able to order the US Government to cease and desist exercising such powers.