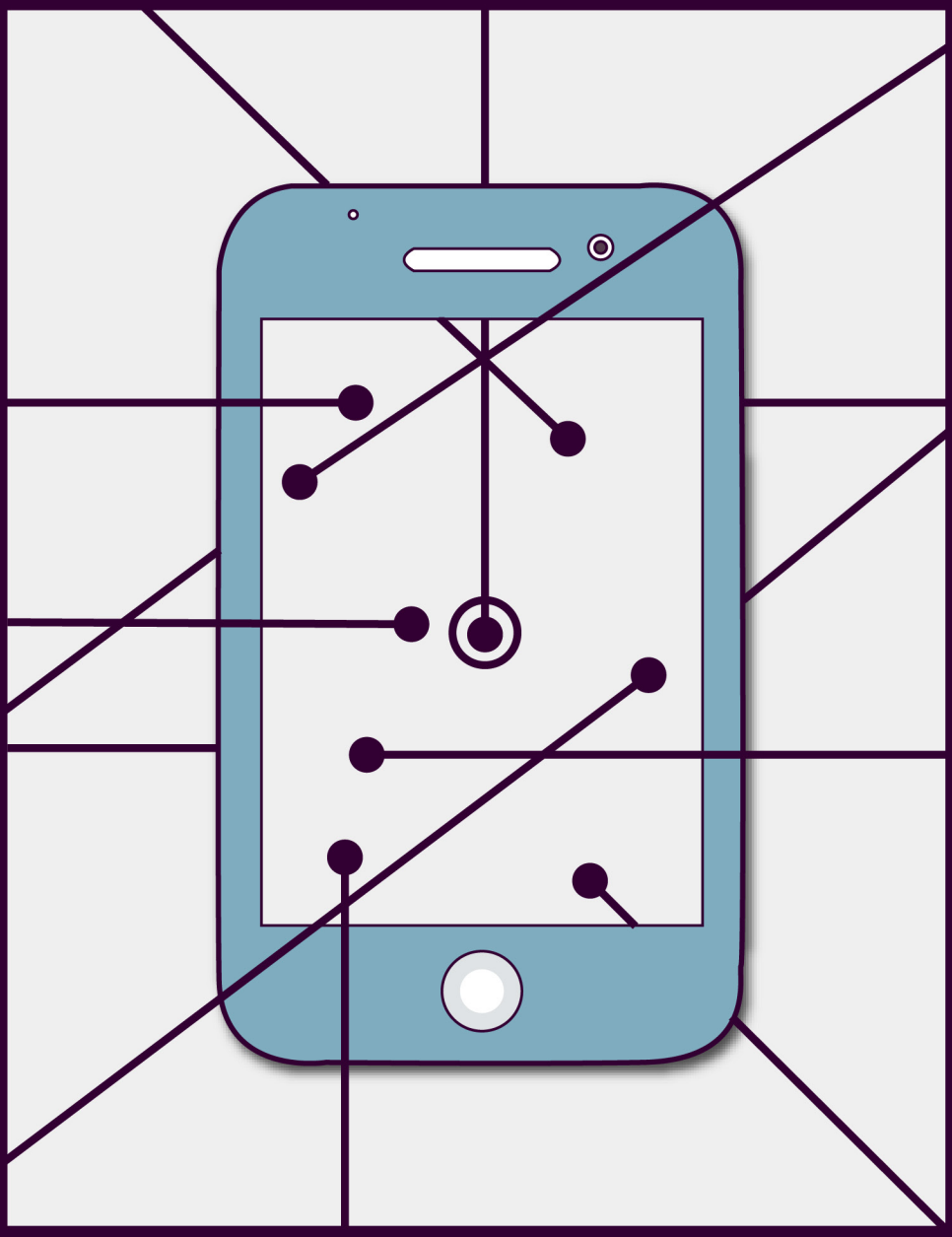
Electronic Devices Privacy Handbook

A GUIDE TO YOUR RIGHTS AT THE BORDER



BCCLA

CIPPIC

Important Notice

This handbook has been prepared and published for educational and discussion purposes only. It is not legal advice and it is not intended that this handbook should in any way replace legal advice from a qualified lawyer. Individuals with specific legal problems should seek advice from a qualified lawyer.

Thanks to the Canadian Internet Registration Authority for its financial support that made this project possible.

BC Civil Liberties Association
306 – 268 Keefer Street
Vancouver, BC V6A 1X5
www.bccla.org

Canadian Internet Policy and Public Interest Clinic
100 Thomas More
Suite 306, Brooks Building
Ottawa, Ontario
www.cippic.ca

Written by BCCLA, CIPPIC, and Greg McMullen, with support from Sancho McCann, Graeme Cook, Lex Gill (Citizen Lab), and Seth Schoen (Electronic Frontier Foundation).

Design & Cover by BC Civil Liberties Association, 2018

Electronic Devices Privacy Handbook

A GUIDE TO YOUR RIGHTS AT THE BORDER

Contents

PHOTO CREDIT: WARREN WONG

CHAPTER ONE

Overview

More and more of our lives involve interacting with an electronic device. You use a laptop for work or school, text message your friends and family, check Facebook on your iPad, take hundreds of photos on your camera phone, read books on your e-reader, and send emails from whatever device you happen to have with you at the time.

When you slip your smart phone into your pocket or laptop into your bag, it is easy to forget the volume of information you're carrying with you. It could easily be the digital equivalent of an entire filing cabinet. For many people, it is an entire library – years of correspondence, business records, personal conversations, photos, web surfing history, banking information, and reading habits – all stored on one device.

The idea of someone digging through all that information and deciding if you should be allowed to come into Canada or not seems implausible, but that is exactly what happens when the Canada Border Services Agency (the "CBSA") searches electronic devices at the border.[1]

While you may feel like you have nothing to hide, you probably do not want a stranger reading through years of your personal emails or texts, looking at pictures of your kids in the bathtub, seeing when your next scheduled medical checkup is, examining your web browser history, or browsing your tax returns – all examples of the kind of data that many of us keep on our electronic devices. This is especially true if you have confidential business records or client data. The concerns are bigger still if you are a doctor with patient information, a journalist with sensitive sources, or a lawyer with privileged client information on your phone or laptop.

The law around searches at the border was designed during a time when people would only bring a small amount of personal information with them, but seem out of date in a time when someone can bring vast troves of personal data about them along in their pocket. This handbook is meant to help you make sense of the current state of play with respect to electronic searches at the Canadian border and at US preclearance zones in Canada, and to protect your privacy when travelling with electronic devices.

1 In this guide, borders refer to ports of entry that are staffed by CBSA and include land border offices and airports.

What This Guide Does

This guide will explore these areas:

01	**Rights at the Canadian border** – What can and can't be done by a CBSA officer when they decide to search your electronic devices?
02	**CBSA policies** – What exactly do CBSA officers do when they are searching your electronic devices?
03	**Rights at U.S. preclearance areas** – What can and can't be done by a pre-clearance officer when they decide to search your electronic devices?
04	**Best practices** – What steps can you take to keep your data private and secure?
05	**I've been searched!** – What should you do if your electronic devices have been searched by the CBSA?

With this helpful guide, you will be as ready as you can be for your next border crossing.

What This Guide Does Not Do

This guide does not replace your lawyer. Nothing here is legal advice. If you have serious concerns about the security of your data while crossing the border or have other legal issues that need to be addressed, go talk to a lawyer and find out how the law applies to your particular situation.

The CBSA does not publish its policies, so the information presented here may already be out of date. Expect the unexpected!

Finally, this information only applies to crossing the border into Canada or out of Canada through US preclearance areas. Other countries have different policies.

CHAPTER TWO

Your Rights at the Border

Your rights when crossing the border are very different than your rights when walking down the street.

While the Charter of Rights and Freedoms (the "Charter") still applies while you are at a border crossing, Canadian courts have found that the government's interest in keeping dangerous goods and undesirable people out of the country gives the CBSA more power to search people and their possessions than police have in other settings.

Although Canadian courts are increasingly aware of the unique concerns that electronic devices pose for privacy, judges continue to uphold the customs searches as reasonable when challenged by defense arguments to the contrary.

The bottom line is that the CBSA can and does search electronic devices at the border, both randomly and specifically for individuals who meet certain criteria. This section will explore the powers of the CBSA to conduct searches of electronic devices crossing the border.

PHOTO CREDIT: BC EMERGENCY PHOTOS

The Customs Act

The *Customs Act* gives the CBSA broad powers to search both people and goods coming into the country.[2] This includes the things that people bring with them, even the files on your electronic devices.

The CBSA has the power to search goods coming into Canada without a warrant. [3] This is true even if the CBSA has no reason to suspect that the goods are or contain contraband. Canadian courts have found that the government has an interest in controlling what and who comes into the country, so the rights to privacy that we enjoy within Canada's borders do not exist at the border itself.

The *Customs Act* makes it clear that border officers have the ability to search "any document in any form" – including electronic documents.[4]

Canadian courts have found that files stored on electronic devices count as goods under the *Customs Act*, and that the CBSA has the power to search these documents.[5]

CBSA documents show that it treats computer files the same way it would treat a box of documents, claiming that "the only difference between a paper document and information stored electronically is the medium it is stored on."[6]

2 Customs Act, RSC 1985, c 1 2nd Supp. Section 99(1) allows a CBSA officer to examine any goods that have been imported and s 99.3(1), which allows a CBSA officer to conduct a "non-intrusive examination of goods in the custody or possession of a person who is in or leaving a customs-related area." Most jurisprudence regarding the search of electronic devices revolves around s 99(1) but some cases have instead interpreted s 99.3(1).

3 See e.g. R v Saikaley, 2012 ONSC 679 ("the Applicant's iPhone. . . is included in the definition of 'goods'" at para 102); R v Buss, 2014 BCPC 16 ("While I am told that no court in B.C. has specifically considered whether a computer or a cell phone is a "good" under the Customs Act, I find that both are" at para 25); R v Moroz, 2012 ONSC 5642 ("the expression 'goods' . . . reflect[s] the type of information found in electronic devices such as a cell-phone or an I-Phone." at para 20); R v Whittaker, 2010 NBPC 32 ("[A] computer file such as the digital storage of photographic images is a document and falls squarely within the definition of 'goods'" at para 8); R v Appleton, 2011 CarswellOnt 11191, 97 WCB (2d) 444 (Ont SCJ) ("The texts may not be goods in themselves, but could be located while on a search for goods." at para 12).

4 Customs Act, supra note 2.

5 See e.g. R v Leask, 2008 ONCJ 25; R v McDermin, 2008 CanLII 68135 (Ont SCJ); R v Whittaker, supra note 3; R v Gibson, 2017 BCPC 237.

6 Canadian Border Services Agency, Access to Information Request Response Volume 2 (3 May 2010) British Columbia Civil Liberties Association (blog), online: <https://bcclanationalsecurity.files.wordpress.com/2010/03/a-2009-01850-vol2.pdf> at 5 [CBSA ATI Vol 2]. In 2009, the BCCLA made a request for documents from the CBSA under the Access to Information Act. The BCCLA asked for policies on the search and inspection of electronic devices, statistics on the number and kind of devices searched, criteria used to select people for device inspection, policies for requesting and requiring passwords from individuals, and other information. The CBSA

So far, Canadian courts have agreed with the CBSA. Despite the clear differences between the few paper documents in a travellers' briefcase and the nearly limitless volumes of documents that can be stored on an electronic device, the few attempts to argue around this assessment have so far failed. [7]

The Immigration and Refugee Protection Act

The *Immigration and Refugee Protection* Act is the primary federal legislation that governs immigration to Canada. Under this statute, a CBSA officer may search the "luggage and personal effects" of a person seeking to come to Canada where an officer has reasonable grounds to believe that the person has not revealed their identity or has hidden, on or about their person, documents that are relevant to their admissibility.[8] A CBSA officer may also search the "luggage and personal effects" of a person seeking to come to Canada if there are reasonable grounds to believe that the person has committed, or possessed documents that may be used in the commission of people smuggling, human trafficking, or document fraud. [9]

A CBSA Operational Bulletin current to 2017 makes it clear that "electronic devices and media" are interpreted as "personal effects" and thus searchable under these statutory powers.[10] Searches of devices and media "must be confined to identifying the person, finding documents relevant to admissibility or that may be used in the specific offences, or finding evidence of the specified offences."[11]

---

replied in early 2010, providing the BCCLA with several volumes of documents. While not all of our questions were answered, the documents helped develop our picture of how the CBSA conducts searches of electronic devices. Full details of the request and the response provided by the CBSA is available on the BCCLA National Security Blog, along with links to each volume: Carmen Cheung, "CBSA laptop search documents" (3 May 2010) British Columbia Civil Liberties Association (blog), online: <http://bccla.org/2010/05/cbsa-laptop-search-documents> [CBSA search documents].

7 R v Leask, supra note 5 at para 100.

8 Immigration and Refugee Protection Act, SC 2001, c 27, s 139(1)(a) [IRPA].

9 Ibid, s 139(1)(b).

10 Canada, Parliament, House of Commons, Standing Committee on Access to Information, Privacy and Ethics, Protecting Canadians' Privacy at the US Border: Report of the Committee, 42nd Parl, 1st Sess, No 10 (December 2017) (Chair: Bob Zimmer), online: <http://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9264624/ethirp10/ethirp10-e.pdf> at 24 [Privacy at the US Border].

11 Ibid.

Search Without Suspicion

A suspicionless search is any search that occurs without a reason to believe that the goods being searched are illegal. A suspicionless search may be totally random, or it may be based on the officer's hunch that something is not quite right.

Usually, police cannot randomly search individuals in Canada. This is due to the protection against unreasonable search and seizure that is provided by the Charter.[12]

This is not the case during a border crossing.

At the border, the CBSA can search anything carried by a person. In the past, this has included brief pat downs of a travellers' clothing,[13] detailed searches of luggage,[14] or reading a traveller's bankbook.[15] The CBSA can use this power to search electronic devices and the files on them.

More information about the kinds of searches conducted by the CBSA and the methods its officers use when searching electronic devices can be found in Chapter 3 – CBSA Policies.

Limits to Suspicionless Searches

Even though the CBSA can search your electronic devices without a warrant or even suspicion, there are limits to these searches.

To date, no court cases have put limits on the searches of electronic devices that can be conducted by the CBSA. However, the CBSA documents obtained by the BCCLA indicate that the CBSA hopes to avoid challenges to their search powers, so may be limiting searches to what they believe is allowed by the Charter.[16]

CBSA training manuals make it clear that during a suspicionless search, officers are not to go into great detail reading every single document or looking at every single photo on your electronic device.[17] Officers can only look

12 Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11, s 8.

13 R v Simmons, [1988] 2 SCR 495, 1988 CanLII 12 at para 84.

14 R v Hardy, 1995 CanLII 1520, 103 CCC (3d) 289 (BCCA).

15 R v Jones, 1992 CanLII 1096 (BCSC).

16 Canadian Border Services Agency, Access to Information Request Response Volume 9 (3 May 2010) British Columbia Civil Liberties Association (blog), online: <https://bcclanationalsecurity.files.wordpress.com/2010/03/a-2009-01850-vol9.pdf> at 36-37 [CBSA ATI Vol 9].

17 Canadian Border Services Agency, Access to Information Request Response Volume 4 (3 May 2010) British

at documents for long enough to determine that they do not contain contraband such as child pornography or hate literature. This means they can take a quick look at each before moving on to the next document.

Information found during a suspicionless search can be used to justify a more detailed search. For example, during a search of a suitcase, a CBSA officer found unusual glue marks around the liner of the case. This was enough to justify a more detailed search that included emptying the suitcase, then subjecting the search to an x-ray, and finally drilling into the suitcase.[18] The BC Court of Appeal found that while drilling into a random suitcase to look for drugs may not be permissible under the Charter, the suspicion raised in the earlier searches made it reasonable.

The same idea also applies in the digital world. If a CBSA officer finds things on your electronic device that leads them to believe that you may have contraband or have otherwise committed an offence, they may perform a more detailed search. While they may not have to physically drill into your laptop to find the data they are looking for, the comparison is a good one. They will look beyond the most obvious layers of information to see what is hidden away deeper in your electronic device.

Racial and Religious Profiling

We are concerned that travellers are targeted for searches based on markers such as race or religion, and that such profiling can masquerade as a random search. Although any such profiling would be a breach of the law, it is extremely hard to prove discrimination. This is why we have long been advocating for effective oversight, review and data gathering mechanisms for the CBSA.

Columbia Civil Liberties Association (blog), online: <https://bcclanationalsecurity.files.wordpress.com/2010/03/a-2009-01850-vol4.pdf> at 10, s 42 [CBSA ATI Vol 4].

18 R v Sekhon, 2009 BCCA 187 at para 91.

Summary

When you are crossing the border, if the CBSA decides to search your electronic devices, there is little that you can do about it. The most secure way to protect your privacy and the contents of your electronic devices has to be done before you get to the border. The rest of this guide is meant to help you do just that. The next chapter will tell you what you can expect from a search by the CBSA. The last chapter will tell you what steps you can take to keep your data out of the hands of the CBSA if you do get searched.

PHOTO CREDIT: ALEJANDRO MOLINA FERNANDEZ

CHAPTER THREE

CBSA Policies

While detailed information about CBSA policies for searches of electronic devices is still limited, requests made in recent years under access to information law shed some light on the subject. These documents provide information on how the CBSA chooses people to search, how those searches *should* done, and what happens to the data they collect.[19] Much of this chapter is based on a CBSA Operational Bulletin regarding the examination of electronic devices and media at the port of entry that was made available in 2017 to the public in a parliamentary report.[20]

Please note that guidelines, policies, bulletins, manuals and other kind of procedural documents used by the CBSA *do not have the force of law*. These materials are intended to provide guidance to CBSA staff about how the legal instruments described in the last chapter (i.e. the Charter, *Customs Act* and *Immigration and Refugee Protection Act*) should be interpreted and applied in daily operations. Although these documents may appear to the public as binding rules, they are not legal standards that a person could seek to enforce in a court.

No Access to Remote Data

The CBSA has the no authority under the *Customs Act* to search data that is not already on an electronic device.[21] In testimony to a House of Commons committee, a CBSA representative claimed that their staff should not ask a person to activate WiFi during an examination. If the CBSA wants to search information on the phone that is only accessible once it is connected to the cloud, they said, the agency must first obtain a warrant issued by a judge. [22]

19 Cheung, supra note 6.

20 Privacy at the US Border, supra note 10.

21 R v Gibson, supra note 5 at para 92.

22 Canada, Parliament, House of Commons, Standing Committee on Access to Information, Privacy and Ethics, Evidence, 42nd Parl, 1st Sess, No 69 (27 September 2017) at 1, online: <http://www.ourcommons.ca/Content/Committee/421/ETHI/Evidence/EV9117508/ETHIEV69-E.PDF> [ETHI Evidence].

This approach is reflected in CBSA policy; officers are directed not to search online accounts or information that is not already stored on the device.[23] Officers should set the device to airplane mode prior to searching to "reduce the possibility of triggering remote wiping software, inadvertently accessing the Internet or other data stored externally or changing number versions or dates."[24] For emails, this means that the officers can only read those which have already been downloaded on the device and opened, and they asses this by seeing whether the emails have been marked as read.[25] Presumably, the same approach applies to text messages.

Level One: Initial and Progressive Searches

The CBSA can and does search electronic devices, including laptop computers, cellphones, cameras, smartphones, and storage mediums like USB flash drives. The CBSA recognizes that examining electronic devices is more personal than baggage examinations, and directs officers to conduct their searches "with as much respect for the traveller's privacy as possible."[26]

Nevertheless, the agency maintains that it has the authority under the *Customs Act* to search electronic devices without suspicion.[27] It says, however, that the examination of electronic devices and media should always be done with a "clear nexus" to administering and enforcing laws about the cross-border movement of people and goods, plants and animals.[28] CBSA officers are also directed not to

23 R v Gibson, supra note 5 at para 92.

24 Privacy at the US Border, supra note 10 at 25.

25 Ibid.

26 Ibid.

27 Ibid at 23.

28 Ibid at 24.

examine electronic devices "with the sole and primary purpose of looking for evidence of a criminal offence under any Act of Parliament."[29]

Despite the lack of a legal threshold for grounds to examine such devices, the current policy of the CBSA is to discourage routine examinations; an officer should only search the contents of the electronic device "if there is a multiplicity of indicators that evidence of contraventions may be found" on the device.[30] The CBSA uses the notion of "indicators" to describe warning signs, or clues, of non-compliance.

Front line CBSA officers can conduct initial searches of electronic devices. For the most part, this is done using the software already installed on the electronic device to search out and browse through images, videos, and other files. This browsing is supposed to be a quick peek rather than a thorough review.[31]

If the CBSA officer sees something that they feel needs a closer inspection, a slightly more thorough search may be conducted. This is not a forensic evidence-gathering mission. For example, a CBSA officer may find a receipt on the device that refers to the acquisition or origin of goods that could provide evidence of a contravention of the *Customs Act*. The search of the device may only progress if new indicators emerge or there is a discovery of undeclared, prohibited, or falsely reported goods.

When CBSA officers do search electronic devices, they are expected to take notes about all the indicators that led to the progressive search of the device or media.[32] The officers should be able to explain how they expect each document, application, or program they examine to be relevant to verifying their concerns.[33]

CBSA officers may look for child pornography or hate literature on electronic devices and media. However, the CBSA does not have the best track record with distinguishing between legal and illegal pornography, and has been

29 Ibid.

30 Ibid at 23.

31 CBSA ATI Vol 9, supra note 16 at 2 slide 5.

32 Privacy at the US Border, supra note 10 at 25.

33 Ibid.

known to seize pornography that is completely legal.[34]

Sometimes, CBSA officers will look for other documents as well, including documents that show political opinion. For example, Amy Goodman, an American journalist was questioned extensively about a speech that she was coming to Vancouver to give before the 2010 Winter Olympics. As a part of her examination, the CBSA searched her electronic device.[35]

Where a CBSA officer uncovers evidence of a criminal offence while conducting a search of an electronic device or media, that officer must "be cognizant of where the regulatory examination crosses over to the realm of a criminal examination" and must consult with their supervisor and determine whether to continue the exam based on the context.[36]

34 Little Sisters Book and Art Emporium v Canada (Commissioner of Customs and Revenue), 2007 SCC 2.

35 "US journalist grilled at Canada border crossing", CBC News (26 November 2009), online: <http://www.cbc.ca/news/canada/british-columbia/u-s-journalist-grilled-at-canada-border-crossing-1.801755>.

36 Privacy at the US Border, supra note 10 at 24-25.

PHOTO CREDIT: RAHUL CHAKRABORTY

Level Two: Detailed Searches

CBSA officers with special training in the handling of electronic devices are put in charge of detailed searches. They use special forensic tools to ensure that evidence is not corrupted or lost in the process of the search.

From the CBSA documents the we have seen, you will probably know if your device is being subjected to a thorough search. Your device will be taken out of your possession and brought to CBSA specialists behind the scenes. You may be asked for your username and password. See the password section of this guide for further information about this.

CBSA specialists use a variety of techniques to search electronic devices, including the copying of data from your electronic device. The *Customs Act* gives the CBSA the power to detain goods if the officer is not satisfied that the goods have been properly screened for admission into Canada. This includes the contents of electronic devices.

The CBSA's electronic search experts can make exact duplicates of everything on your electronic device. These duplicates, known as disc images, allow for later inspection of everything that is on the drive. If the inspection is carried out properly, the duplicated results can be used as evidence in court if you are charged with an offence under the *Criminal Code*, the *Customs Act*, or other laws.[37]

Taking disc images also allows the CBSA to run password-cracking software to try and access any data you did not provide a password to access. Over a long enough timeframe any password can be broken, but using a strong password makes the process much more time consuming, to the point that it is all but impossible. An extremely strong password can take hundreds of years to break, even on the best supercomputers.

Tips on picking a strong password are below, in Chapter 5 – Best Practices. Not every border crossing has computer search specialist on staff. Often, electronic devices will have to be detained to give the officer time to conduct a full search of the device. However, CBSA officers have been trained to return electronic devices as quickly as possible to avoid challenges to current

37 CBSA ATI Vol 9, supra note 16 at 36-37.

CBSA practices. Unfortunately, this will often mean that data is copied for later inspection. In our experience, however, detentions of electronic devices by CBSA can last for months.

Random Searches

In theory, random searches are just that – random. Even if you do not fit the profile of someone who is more likely to be searched, your electronic device may be searched all the same.

PHOTO CREDIT: FANCY CRAVE

Targeted Searches

Most of the people searched by the CBSA are not chosen at random, but rather through the National Targeting program or through the application of various criteria (referred to as indicators) that the CBSA feels increases the likelihood that a person's electronic devices will contain some form of contraband, such as child pornography or hate literature, or evidence of a crime.

National Targeting Program

Travellers arriving in Canada via commercial airlines, rail and cruise ships have their passenger information provided to the government of Canada by the carrier in advance of their arrival. This data is used by the CBSA's National Targeting program to "push the border out" and identify potential high-risk travellers prior to their arrival at the border.[38] The program was established in 2014 and uses methodologies that are aligned with the US.

The information about a person that is analyzed is the Advance Passenger Information (API) and Passenger Name Record (PNR) data that all commercial carriers are required to send to CBSA under law. The API includes full name, date of birth, gender, citizenship or nationality, travel document type, number and country of issue, reservation record locator number and passenger reference number. The PNR information may include ticketing information, baggage information, address, contact phone numbers, seat number and payment information.

This information is uploaded[39] to the Passenger Information System (PAXIS) and algorithms are used to match individuals against scenarios for further risk assessment. Scenarios are used to assess travellers for what are considered predictive risk factors in areas such as immigration

38 Canada Border Services Agency, 2016–17 Report on Plans and Priorities (Ottawa: Minister of Public Safety and Emergency Preparedness, 2016), online: <https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/rpp/2016-2017/rpp-2016-2017-eng.pdf> at 8 [CBSA Report 2016].

39 Both the Customs Act, supra note 2, s 107 and IRPA, supra note 8, s 148(d) authorize the use of passenger information for this purpose.

fraud, smuggling of contraband, terrorism and organized crime. These scenarios are not publicly available, for security reasons.[40]

If a passenger is flagged by the system, a National Targeting Centre (NTC) officer conducts a further risk assessment of that individual. As a part of this process, the passenger information is shared with US. border authorities. The NTC officer may also search national and international databases, a review of tax records and social media. The NTC officer may also consult with domestic law enforcement agencies and intelligence agencies about the individual.

A "target" is issued for a traveller if the NTC officer determines that the person may be a risk.[41] Targeted travellers will be subject to questioning and possibly further examination by CBSA once they arrive at the Canadian Port of Entry.

Of the 29 million travellers who arrived in Canada by commercial air carrier in 2016-17, approximately 60,000 (0.02%) of travellers were flagged under the SBT.[42] Of these, 552 travellers were identified for further examination upon arrival in Canada. This represents 0.002% of travellers in that calendar year.[43]

40 Office of the Privacy Commissioner of Canada, Canada Border Services Agency – Scenario Based Targeting of Travellers – National Security (21 September 2017) at para 8, online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/audits/ar-vr_cbsa_2017>.

41 Ibid at para 7.

42 Ibid between paras. 30 and 31 (CBSA response).

43 Ibid between paras. 30 and 31 (CBSA response).

Multiplicity of Indicators

The CBSA uses indicators to detect non-compliance at the border. In a 2017 court case, a CBSA Director testified that "typically electronics will be examined if a multiplicity of indicators has been developed that gives rise to a reason to look at the electronic device."[44] There is no publically available list of the indicators that the CBSA uses to detect non-compliance, but we have gathered a list of some known indicators gleaned from news stories, policy documents and court cases. Note that not all indicators are catalogued by the CBSA in writing; indicators may in part depend on the experience of the CBSA agent.[45]

You are more likely to be chosen to have your devices searched if you:

- Are importing something the CBSA deems to be suspicious.[46] This could include anime and manga, which the CBSA is highly suspicious of. The CBSA has reminded its officers that "most [anime and manga is] not child porn".[47]
- Have travelled to and from "high risk" destinations.[48] A list of high risk destinations has not been provided by the CBSA. However, news reports suggest that the list may include Southeast Asia, Germany, Cuba[49] and Spain.
- Are a single man traveling alone.[50]

44 R v Canfield, 2017 ABQB 350 at para 42.

45 Ibid at para 46.

46 CBSA ATI Vol 4, supra note 17 at 6 s 32.

47 Canadian Border Services Agency, Access to Information Request Response Volume 6 (3 May 2010) British Columbia Civil Liberties Association (blog), online: <https://bcclanationalsecurity.files.wordpress.com/2010/03/a-2009-01850-vol6.pdf> at 13 [CBSA ATI Vol 6].

48 CBSA ATI Vol 4, supra note 17 at 6 s 32.

49 R v Canfield, supra note 44 at para 56.

50 "Pope appoints new bishop for troubled N.S. diocese" Hamilton Spectator (21 November 2009), online: <https://www.thespec.com/news-story/2193795-pope-appoints-new-bishop-for-troubled-n-s-diocese/>.

- Demonstrate "an interest in Pornography".[51] This means pornography in general, not child pornography.
- Are associated, or are believed to be associated, with known importers or exporters of materials the CBSA objects to.[52]
- Exhibit nervousness, agitation, are talking fast, contradicting oneself.[53]
- Have multiple electronic devices (including hard drives).[54]
- Purchase a ticket to travel at the last minute, within days of departing for the trip.[55]
- Are hesitant in answering questions.[56]
- Have coding on your suitcase that doesn't match where you are coming from.[57]
- Have "unusual" travel routes (e.g. travelling to Canada from Illinois by car but only crossing the border in Vancouver).[58]
- Have file names associated with pornography (the discovery of a progressive search.[59]

51 CBSA ATI Vol 9, supra note 16 at 3 slide 9.

52 CBSA ATI Vol 4, supra note 17 at 6 s 32.

53 R v Canfield, supra note 44 at paras 35 and 53.

54 Ibid at para 53.

55 Ibid at para 56.

56 R v Buss, supra note 3 at para 12.

57 ETHI Evidence, supra note 22.

58 R v Gibson, supra note 5 at para 7.

59 R v Mozo, 2010 CarswellNfld 447, [2010] NJ No 445 at para 4.

CBSA Data About Number and Location of Searches

Until recently, the CBSA did not record information about the number of inspections of electronic devices or the types of devices checked. They started to record this information in 2017 and have committed to making the results publically available.[60]

Initial data from the CBSA about such examinations has been made available through an access to information request.[61] The information is limited to a period of 16 weeks and indicates that about 40 electronic devices, on average, are "examined" each day.[62] Of these devices that are examined, an average of 13 are "searched."[63] It is unclear what the difference between an "examination" and a "resultant search" is, as these terms are not reflected in the law or policy. It may be that an examination refers to what this guide calls an initial search while a "resultant search" may correspond to what this guide refers to as a detailed search.

Interestingly, 57.36% of the examinations took place in British Columbia and Yukon (the Pacific region), while only 10.44% occurred in the Greater Toronto Area.[64]

60 ETHI Evidence, supra note 22.

61 Canada Border Services Agency, Statistics from July 1, 2017 to February 19, 2018 pertaining to the search of electronic devices including information about the type of device and the location of where each inspection occurred, Access to Information Request Previously Released A-2018-03264 (March 2018), available upon request online: <https://open.canada.ca/en/search/ati/reference/040b79163c96b8a8b52579f91015806f>.

62 Ibid.

63 Ibid.

64 Ibid.

Passwords

If your electronic devices are searched, the CBSA will ask you to provide any passwords required to access the information on them.[65] Sometimes a password is required to unlock the device itself. Other passwords may be required to open specific software or "apps" on the device.

Device Passwords

There is uncertainty as to whether a person is legally required to disclose a device password to a CBSA officer if asked to do so. There is an obligation under the *Customs Act* for a person to "answer truthfully any question asked by an officer with respect to the goods" and to "open or unpack any package or container that the officer wishes to examine." [66] A CBSA officer also has the power to arrest a person at the border for "hindering"[67] or "obstructing"[68] an officer in the performance of their duties.

The issue is muddled because the question has yet to be directly considered by a court, and a recent interim policy (no longer in effect) asked the CBSA not to make such arrests. One legal scholar has argued that there is no statutory authority to arrest someone for hindering or obstruction, given that the offence is tied to hindering a search for "imported goods", and a traveller's electronic device is usually neither "imported" nor a "good" in the proper senses of those words.[69] However, a court has said in passing that a person is subject to arrest if they don't reveal their password,[70] and in *Whittaker*, the CBSA used the threat of arrest for hindering to get the traveller to provide his password, and the court took no issue with it.[71] There is also one known case in which the CBSA

65 CBSA ATI Vol 9, supra note 16 at 3 slide 9.

66 Customs Act, supra note 2, s 13.

67 Ibid, s 153.1.

68 IRPA, supra note 8, s 129(1)(d).

69 Robert J Currie, "Electronic Devices at the Border: The Next Frontier of Canadian Search and Seizure Law?" (2016) 14:2 CJLT 289.

70 R v Canfield, supra note 44 at para 44.

71 R v Whittaker, supra note 3 at para 4.

arrested a traveller when he failed to reveal his electronic device password.[72] CBSA "interim" guidelines that were in effect from mid-June 2015 until an unknown recent date directed officers not to make such arrests. The policy had said that "[t]hough such actions appear to be legally supported, a restrained approach will be adopted until the matter is settled in ongoing court proceedings." [73]

The current policy is completely silent on whether or not a CBSA officer may arrest a person if they don't share a device or media password when asked to do so. Recent testimony by a CBSA representative in front of a parliamentary committee revealed that if a person refuses to disclose a password, the CBSA acts on a case-by-case basis. They maintain that because individuals have an obligation under the *Customs Act* to present and open goods if requested to do so by an officer, and a password may be required to open and access documents on an electronic device, that an officer has the authority to compel a traveller to provide it. [74] In most cases, people at the border cooperate and provide a password. The CBSA maintains that an "officer may order the disclosure of the password and, if the person refuses and the officer has good reason to believe that there may be prohibited material on the phone, there may be an arrest and perhaps even an appearance in court." [75]

What is more clear is that CBSA officers will likely only request passwords required to gain access to information or files that are known or suspected to exist within the electronic device or media being examined. CBSA officers should not compel passwords to gain access to any account, file or information that might potentially be stored remotely or online. [76]

72 Brett Ruskin, "Alain Philippon pleads guilty over smartphone password border dispute" CBC News (15 August 2016), online: <http://www.cbc.ca/news/canada/nova-scotia/alain-philippon-to-plead-guilty-cell-phone-1.3721110>.

73 Canadian Border Services Agency, Access to Information Request Response Volume 11 (August 2016) online: <https://bccla.org/wp-content/uploads/2016/08/CBSA-FOI-Docs.pdf> at 5 [CBSA ATI Vol 11].

74 ETHI Evidence, supra note 22.

75 Ibid.

76 Ibid.

What to Expect if You Provide Passwords(s)

If you do give your password to the CBSA, you will not be able to input it yourself unless the device is biometrically protected (i.e. fingerprint). In such cases, the officer is supposed to control the device by holding it and is expected to monitor it while the traveller allows the device to read their fingerprint.[77]

With non-biometric passwords, CBSA officers are to request the password to access the device and to record the password and alternate passwords in their notebook.

Password protections are to be deactivated by a CBSA officer as soon as they find evidence of a contravention on the device or media.

What to Expect if You Do Not Provide Password(s)

It is difficult to predict exactly what a CBSA officer will do if you do not provide a password. This is due to the legal uncertainty and the many possible contexts in which a traveller may be asked for a password. Here are some possible consequences that you should consider when deciding whether or not to offer up your password(s).

Increased Suspicion

The CBSA may treat a refusal to provide a password as suspicious, and inspect your electronic device more carefully or ask probing questions.

Denial of Entry

If you are not a Canadian or a permanent resident, there is a risk that you will be denied entry into the country if you do not cooperate with the CBSA.

Detention of the Device

The CBSA has the power to detain goods entering the country for inspection if they are not able to determine that the goods should

77 Privacy at the US Border, supra note 10 at 25.

be able to enter the country.[78] This power can be used to keep electronic devices for more detailed inspection by the CBSA's electronics experts, which can take months.

CBSA policy is also clear that if because of not having a password (or for unrelated technical difficulties) an officer cannot complete inspecting a device, the device could be detained and sent to a specialist for a forensic examination.[79] So a traveller risks losing access to their device, usually for a considerable time, if they withhold the password.

A recent court decision, however, suggests that detaining an electronic device for a full forensic search is tantamount to a seizure and is thus illegal absent reasonable suspicion. While an electronic device may be detained by CBSA "over a period of time that is not brief" [80] until an officer is satisfied that the good has been dealt with in accordance with the *Customs Act*, such a search is limited to the extent that the "electronic device is not subject to the level of scouring that may take place when such a device is seized, reviewed, imaged and examined in the course of a full forensic search."[81]

Arrest

As described above, you could be arrested for hindering or obstructing a CBSA officer. A person convicted of this offence could face a fine of up to $50,000 and/or a term of imprisonment for five years.[82]

78 Customs Act, supra note 2, s 101.

79 CBSA ATI Vol 11, supra note 73 at 6.

80 R v Gibson, supra note 5 at para 188.

81 Ibid.

82 Customs Act, supra note 2, s 153.1 and IRPA, supra note 8, s 129(1)(d).

What Happens with the Electronic Device Data Collected by the CBSA?

Although the CBSA doesn't publicize how and with whom they share information collected during border searches, a variety of laws and policy suggest that the information gleaned from an electronic device search may be shared with other government agencies, foreign governments and even parties to civil litigation, depending on the context.

The *Privacy Act* applies to the CBSA and requires that personal information under their control shall not be disclosed without the consent of the individual to whom it relates.[83] There are a number of exceptions to this rule, however, including disclosure in accordance with another Act of Parliament.[84] The *Customs Act*, for instance, allows the disclosure of information collected by CBSA without the consent of the individual to whom it applies in a variety of contexts,[85] including to prepare for criminal proceedings.[86] A Memorandum of Understanding between the RCMP and the CBSA suggests that if the RCMP issues a "lookout" in relation to an individual traveller, the CBSA may refuse to share personal information collected during a customs examination of that person (including data based on a search of their electronic device) with the RCMP "in whole or in part but this information will not be unreasonably withheld by the CBSA."[87]

CBSA may also disclose personal information collected during the examination of a traveller

83 Privacy Act, RSC 1985, c P-21, s 8(1).

84 Ibid, s 8(2)(b).

85 Customs Act, supra note 2, s 107(4).

86 Ibid, s 107(4)(a).

87 Canada Border Services Agency, Instructions issued from June 30, 2015 to May 2, 2017 pertaining to the search of electronic devices or media, the Officer Reference Booklet, and Appendix B to the Customs Enforcement Manual entitled "Offences against a Border Services Officer", Access to Information Request Previously Released A-2017-06905 (February 2018), at Investigations and Referrals Annex, Appendix A-4, 2(2), available upon request online: <https://open.canada.ca/en/search/ati/reference/8e2f7336a89a146edf98d41042faf983>.

PHOTO CREDIT: TYLER LASTOVICH

for the purposes of the *Security of Canada Information Sharing Act* ("SCISA").[88] The basic premise of the *SCISA* is to "encourage and facilitate information sharing between Government of Canada institutions in order to protect Canada against activities that undermine the security of Canada."[89] As defined, this means any activity that "undermines the sovereignty, security or territorial integrity of Canada or the lives or the security of the people of Canada."[90] In a 2017 review of the operationalization of SCISA, the Office of the Privacy Commissioner of Canada found that "virtually all disclosures… to date have been directed to CSIS [Canadian Security Intelligence Service] or the RCMP."[91] The review suggested that the CBSA did not have "controls to help ensure that the information-handling practices related to personal information they were sharing or receiving under SCISA complied with their statutory and policy obligations regarding privacy."[92]

The disclosure of personal information by the CBSA to Canadian security agencies such as CSIS and the Communications Security Establishment can in turn lead to the subsequent disclosure of that data to foreign governments.

88 Customs Act, supra note 2, s 107(4)(i).

89 Security of Canada Information Sharing Act, SC 2015, c 20, preamble.

90 Ibid, s 2.

91 Office of the Privacy Commissioner of Canada, Review of the Operationalization of the Security of Canada Information Sharing Act (21 September 2017), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/audits/ar-vr_scisa_2017/>.

92 Ibid at para 36.

We know that Canada has intelligence sharing arrangements with foreign governments, but due to the lack of transparency in relation to such treaties,[93] we are unable to provide any specific guidance about how exactly the data collected from a border search of your electronic device may end up in the hands of a foreign government.

Evidence collected by the CBSA can be used as evidence in other cases, including civil cases. An Ontario court was asked to force the CBSA to hand over a disc image it had taken from an individual to the person suing that individual. In that case, the Court refused to order the CBSA to turn over the data, since the data should have already been destroyed.[94] If the request were made during the period in which the CBSA was allowed to have the data, the CBSA would have been forced to turn over the data. The contents of the defendant's laptop computer could have been used against him by someone other than the government.

According to CBSA policy, copies of data are not retained once the investigation is complete. The CBSA, however, has refused to release information on how data is destroyed after collection, except when goods are made "forfeit" because they contain contraband like child pornography or hate literature. Goods that are forfeit are seized by the CBSA and never returned to their original owners, and would likely be the original devices, not the copies. Once an investigation has been completed and the evidence is no longer needed, the CBSA destroys the electronic devices by "drilling holes into electronic media or discs" and then making sure the data cannot be accessed.[95]

The *Privacy Act* provides people with the general right to gain access to information that is held about them by the federal government, including the CBSA. See Chapter 6 for more information about how to make such a request.

93 Open Letter from Privacy International, BC Civil Liberties Association, Canadian Internet Policy & Public Interest Clinic, Citizen Lab at the Munk School of Global Affairs to Jean-Pierre Plouffe (Commissioner, Communications Security Establishment) and Pierre Blais (Chair, Security Intelligence Review Committee) (13 September 2017), online: <https://cippic.ca/uploads/20170913-LT_re_intel_sharing_agreements-CA.pdf>.

94 Obégi Chemicals LLC v Kilani, 2011 ONSC 4636 at para 33.

95 Canadian Border Services Agency, Access to Information Request Response Volume 5 (3 May 2010) British Columbia Civil Liberties Association (blog), online: <https://bcclanationalsecurity.files.wordpress.com/2010/03/a-2009-01850-vol5.pdf> at 4 [CBSA ATI Vol 5].

CHAPTER FOUR

Preclearance Areas

These are the areas in some Canadian airports, train terminals and ferry terminals where travellers departing for the US clear US customs prior to leaving Canada. To implement an agreement with the US, Canada has provided the legal authority through the *Preclearance Act* for US Customs and Border Protection ("CBP") to operate in these areas as preclearance officers. A new statute was recently passed that will alter the law in these areas and enable preclearance areas to be set up on US soil where CBSA will administer Canadian laws in respect of travellers destined for Canada. This guide will be updated to reflect the new law once it comes into effect.

In a preclearance area, an officer may administer the law of the US with respect to customs, immigration, public health, food inspection and plant and animal health. The administration of these laws are subject to Canadian human rights laws, including the Charter, which means that Canadian search and seizure laws apply in these areas rather than US ones. Although this distinction should provide relief to travellers subject to examination in these areas, it is unclear to what extent preclearance officers working in these zones have knowledge and training of Canadian legal standards with respect to the examination of passengers and their accompanying goods.

Under preclearance law, an electronic device is a "good" and can therefore be examined by an officer. The power of preclearance officers to examine goods under the *Preclearance Act* is essentially the same as the power Canadian CBSA officers have to examine goods under the *Customs Act*.[96] In other words, the officer does not need a warrant or even reasonable

96 United States of America v Amadi, 2017 ONSC 3446 at para 48.

suspicion to examine the information on your electronic device.

The US CBP's 2018[97] Directive on the Border Search of Electronic Devices[98] can help us to understand better how your electronic device may be searched by preclearance officers.

The directive provides that an electronic device search may include searches of information that is already stored on the device itself when it is presented for inspection or when it is detained. CBP officers are to either request that the traveller disable the device's connectivity to any network by putting it into airplane mode, or to put it in this mode themselves. Despite this, the language of the policy does not categorically prohibit the accessing and use of information that may be hosted on a cloud; it says only that a CBP officer cannot intentionally use the device to access information that is solely stored remotely. It also contemplates that an officer will access information "through the device's

97 This is the first policy update since 2009 and is not set for review until 2021.

98 US Customs and Border Protection, "Border Search of Electronic Devices" CBP Directive No. 3340-049A (4 January 2018), online: <https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf> [CBP Search Directive].

operating system or through other software, tools, or applications." [99]

The policy separates device searches into basic and advanced searches. Basic searches can be performed with or without suspicion and involves any search of an electronic device that falls short of an advanced search.

An advanced search is any search in which a CBP officer "connected external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents." These searches require a reasonable suspicion of activity in violation of laws enforced by the CBP, or a national security concern (e.g. individual is on a terrorist watch list).

Travellers have an obligation under the policy to present their devices in a condition that allows the inspection of its contents. If a password is required, the CBP officer may ask you for the password.

What to Expect if You Do Not Provide Password(s)

It is difficult to predict exactly what a US preclearance officer will do if you do not provide a password. This is due to the legal uncertainty and the many possible contexts in which a traveller may be asked for a password.

The law currently says that if a traveller chooses to answer a question, they must do so honestly.[100] The law also provides that the refusal to answer a question is not in and of itself grounds for suspicion that an offence has been committed.[101] If you do not answer a question, the officer may ask you to leave the area and refuse to preclear you for departure to the U.S.[102]

99 Ibid at para 5.1.2.

100 Preclearance Act, SC 1999, c 20, s 16(1).

101 Ibid, s 16(3).

102 Ibid, ss 16(2) and 18.

Detention of Electronic Devices for Continuation of Search

Although the law enables a person to withdraw from this preclearance area without answering a question about your password, the US CBP policy provides that if the CBP officer cannot search the device due to a password or encryption (presumably because the traveller does not facilitate access), the CBP officer can detain the device.

US preclearance officers have the right to detain your electronic device until the officer is satisfied that it has been dealt with in accordance with preclearance laws.[103] If the officer believes on reasonable grounds that the device will provide evidence of an offence under Canadian law, the detention is mandatory.[104] Your electronic device or copies of information contained therein may be detained for a reasonable period of time to perform a thorough border search. Unless there are extenuating circumstances, policy advises that devices should not be detained for more than five days. [105]

If your electronic device is detained, the CBP is supposed to provide you with written notice about the reason and legal authority for the search. The notice should also inform you about how to get more information and how to seek redress from the CBP if you are aggrieved by the search.

Seizure and Retention

A CBP officer may seize your device if in the course of their review of it they determine there is probable cause to believe that the device, or a copy of its contents, provide evidence that you have made a false or deceptive statement.[106]

103 Ibid, s 26(1)(a).

104 Ibid, s 26(2).

105 CBP Search Directive, supra note 98.

106 Preclearance Act, supra note 101, s 27.

PHOTO CREDIT: TYLER LASTOVICH

CHAPTER FIVE

Best Practices

While there are no surefire ways to protect your data when crossing the border, there are a few tips and tricks that can help keep your personal information private and secure.

Where we mention specific proprietary solutions, we only mean these to be examples, not endorsements.

Be aware that a border officer may be annoyed if they realize that a traveller has deliberately tried to thwart a search, especially in a manner that destroys data that the traveller otherwise would have been able to access, or conceals the fact that the data is present at all.

At the end of the chapter, we provide recommendations on how to interact with a border officer[107] should they be interested in examining your electronic device.

Leave Your Electronic Device Behind

The best option for crossing the border is to bring no data at all.

The best way to do this is, if possible, to travel without an electronic device. If you leave your electronic devices at home, there will be nothing for the border officer to search. However, this option comes with the obvious disadvantage of being left without your electronic device once you reach your destination.

107 Border officer refers to either a CBSA officer or a preclearance officer, as the case may be.

Make a Backup

One of the most important things you can do before traveling is to make a full backup of your electronic devices. This backup should not cross the border with you. Making regular backups is a good habit to be in anyhow, in case your electronic device is broken or stolen. However, in the context of a border crossing, it is even more important. A recent backup will make sure you have access to your data if your electronic device is detained for an extended period and gives you the option of deleting unnecessary data from the device you are going to take across the border.

If your backup is stored online, you can even download your data once you reach your destination. Look into whether your online backup storage provider meets your privacy requirements. For example, do they require a warrant from law enforcement agencies before handing over copies of your information?

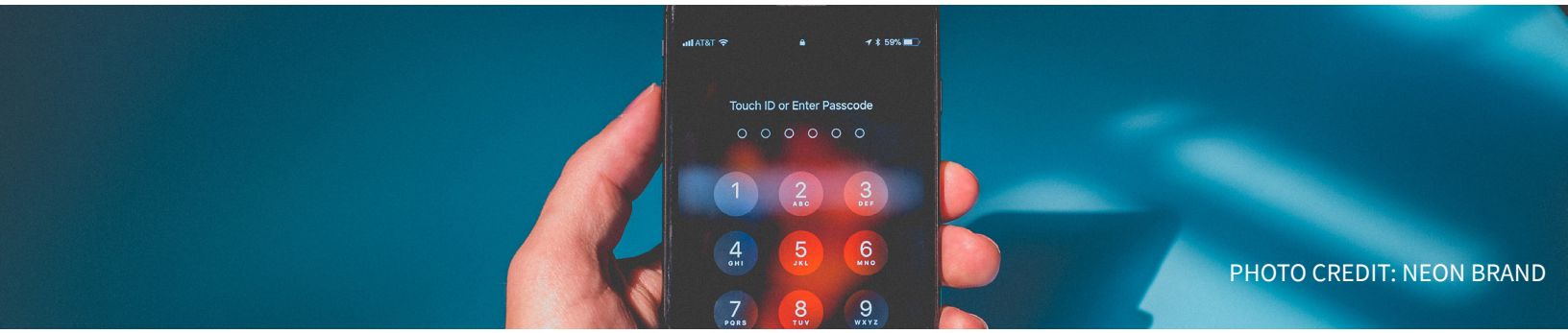
Turn Off Your Devices

Before you are going through customs, turn off your electronic devices. Even if you take all the precautions listed below, security experts have developed ways to access the data stored in your computer's memory while it is powered on. Turning off the computer a few minutes before you go through customs will ensure that these bits of information are cleared.

Getting into the habit of turning off your electronic devices before going across the border will also make sure that you are logged out, and that when a border official turns on your computer, they will need to enter a password before accessing your data as long as you have set up a login password. If you are using full-disk encryption (see below), turning off your device encrypts the device so that your login password will be required to decrypt any content on the disk when it is powered on again.

Note, however, that if you are about to get on a plane, Canadian Air Transport Security Authority (CATSA) officers may require that you turn on any electronic device that is larger than a smartphone as part of "Enhanced Screening."

CATSA is only tasked with inspecting the physical integrity of the device, and will not go through the data stored on it. However, if the device cannot be turned on (perhaps because it is out of battery) or it cannot be removed from its casing, the security officers may prevent you from taking it on the plane.[108]



Require a Login Password

Your first line of defence in protecting against a search of your electronic device is to require a password to log on. This simple step will keep a border officer, or anyone else who wants to access your data, from simply turning on your electronic device and browsing through your files.

Even if you think you would give the border officer your password if asked, it is a good practice to keep your electronic devices password protected. A border officer who is only slightly curious and turns on your electronic device intending to look through it may lose interest when they realize they will have to ask you for your password.

A login password typically goes hand-in-hand with full-disk encryption. A simple screen lock password is not a proper replacement for full-disk encryption. It is simply meant to deter a casual snoop, and can be easily defeated by any experienced forensic examiner. For more information on securing your data with a password, see the sections on full-disk encryption or file encryption, below.

108 Matthew Braga, "Enhanced security for flights to the US: What you need to know" CBC News (19 July 2017), online: <http://www.cbc.ca/news/canada/airport-security-canada-u-s-1.4212727>.

Bring Less Data

If you have made an offline backup or synced your data with a cloud-based storage provider, you may want to delete that information from your device so that it is not with you when you cross the border.

Be aware that border agencies have acquired and potentially use a lot of sophisticated forensic tools, many of which can find data that was once stored on an electronic device that is no longer accessible to an ordinary user. Just because you have pressed "delete" in some interface and can no longer see something does not mean that a border official would not be able to recover at least some portion of that information. Furthermore, if you try to keep your files in cloud storage rather than on your device, there may still be cached copies or deleted copies on your device that could be recovered by forensic tools. There are no tools that we know of that ensure that information is *only* stored on a cloud and that no local copies exist.

With the above caveats in mind, if you do delete files it is important that you delete the data as securely as possible. On many file systems, simply deleting a file doesn't erase its contents from the disk; deletion merely removes the operating system's awareness of the file. If somebody got access to that disk and scanned through it bit-by-bit, they would be able to see the original file unless you securely delete the data or use full-disk encryption.

To securely delete files on Windows, you can use a built-in tool called *cipher*. On OS X, you can use "secure empty trash" or its replacement, *srm*. On linux, two options are *shred* or *srm*. These are not simple tools to use, so full-disk encryption might be preferable, and we advise full-disk encryption for its other benefits anyway.

While wiping your electronic devices clean of data may sound impractical, there are several services that make this much easier than it sounds, especially for devices with smaller capacity, like smartphones.

Most smartphones can synchronize with internet services to download your contacts, calendars, and other information just by entering the password to your account. If you have your data backed up online, you can erase the

information from the device before crossing the border, then enter your password as soon as you clear customs. Within a few minutes your information will be restored.

If you plan to restore the data to your electronic device from the cloud, be careful about data charges, especially when travelling overseas. You may be better off waiting until you have WiFi access rather than using your mobile data provider's connection.

You should also be aware that most cloud backups do not store things like photos, videos, or other locally stored files. These should be backed up separately.

Devices running Google's Android operating system synchronize through Google Accounts, while Apple iOS devices do so through Apple. Android, iOS, and Blackberry devices can all synchronize with Microsoft Exchange servers. These services, and others like them, make it easy to restore data to your smartphone or tablet.

A download of all your data may be less convenient and more time consuming if you are planning on retrieving hundreds of gigabytes of data. If bringing vast quantities of data across the border with you is absolutely necessary, you will want to consider full-disk encryption, which is discussed later.

You can also set up your browsers to store less data to begin with. Most browsers have options that allow you to browse privately (erasing history at the end of a session) and to erase your history and caches.

Keep in mind that storing your data in the cloud may create as many problems as it solves. If your cloud storage provider is located in Canada, Canadian law enforcement can demand a copy of the data with a warrant. If your cloud storage provider is in the US, your data can be accessed under the USA PATRIOT Act without a warrant. Providers like Dropbox keep the encryption key to your data. They can and will turn your data over to law enforcement if it is requested.

If you wish to avoid trusting a cloud provider altogether, you may want to set up your own file-sharing service. One option for this is *ownCloud*. There are tradeoffs, though. Hosting your own file-sharing service puts the burden on you for setup, security, maintenance upgrades, and backups. And, not all ISPs allow you to run your own server over their network.[109]

109 Sophia Cope, Amul Kalia, Seth Schoen and Adam Schwartz, Digital Privacy at the US Border: Protecting the Data on your Devices (Electronic Frontier Foundation, 2017), online: <https://www.eff.org/files/2018/01/11/digital-privacy-border-12-2017.pdf>.

Some organizations do not allow employees to store confidential information in the cloud unless certain precautions have been taken. In British Columbia, government agencies cannot store citizens' personal information on servers located in the US. This would include physicians, who cannot store any patient information outside of Canada. The Law Society of British Columbia has recently drafted guidelines for lawyers using cloud services, and these guidelines may turn into requirements.[110] Before long, lawyers in British Columbia will have to be sure that their cloud service provider offers minimum safeguards for privileged information.

If you are travelling internationally, your mobile phone's data plan may be in roaming mode. You may be charged for every megabyte of data you download. The privacy you gain may come with a steep price tag. Of course, if you are returning to Canada and have a data plan here, this will be much more affordable.

Strong Passwords

Keeping your electronic devices and accounts protected by a strong password is good advice even if you are not crossing the border, but becomes especially important when your electronic devices and data become subject to a border search.

First and foremost, a password is useful only so long as you keep it secret. If you turn your password over to the CBSA, even the strongest password is worthless.

The usual advice for creating passwords is to use random characters, including upper and lower case letters, numbers, and punctuation. Mathematicians and computer security experts have been encouraging a move away from this sort of password, for two reasons. First, it is hard for people to remember the dozens of random passwords they wind up collecting for all their online accounts, meaning that most people re-use passwords. Secondly, computers are now fast enough that breaking what would have been a secure password a few years ago is now trivial.

110 Law Society of British Columbia, "Practice Resource: Cloud computing checklist" (May 2017), online: <https://www.lawsociety.bc.ca/Website/media/Shared/docs/practice/resources/checklist-cloud.pdf>.

Security experts now recommend using a phrase made up of several words in an unusual sequence instead of a single word. This is not only harder for machines to guess, but is also easier for humans to remember.

Sometimes you will not be able to use a passphrase, because many password fields will only accept 8-10 characters. If you cannot use a passphrase, pick a password that is as long as possible and contains upper and lower case letters, numbers, and symbols.

Don't use passwords...

- **That are words in the dictionary or simple combinations of words in the dictionary.** Software can quickly go through long lists of words and common phrases in an effort to guess your password.
- **Based on information that is easily available to potential snoops**, like birthdays, names of family or friends, or your phone number.
- **That you have used for other websites or online services.** Sometimes websites are compromised, and their lists of usernames and passwords posted online. A quick search of your username or email address in these databases could reveal your password if you have re-used it.

If you need help coming up with a strong password, many websites offer password generating tools that mix and match random letters, numbers, and symbols to give a password that meets your needs. This WordPress site is a good resource on creating a strong password and provides links to password generators: https://en.support.wordpress.com/selecting-a-strong-password/

A final option is to not know your password. There are several ways to accomplish this. You could generate a new, random password, and then send it to your destination with somebody else, store it online, or give it to your lawyer.[111]

111 Cope et al, supra note 110.

Two-Factor Authentication

You should be using two-factor authentication to control access to your most sensitive accounts. Two-factor authentication requires you to not only know your password for an account, but to also have access to a physical device that generates a random, one-time-use code each time you need to log in to that account.

PHOTO CREDIT: RAW PIXEL

In the context of a border search, the two-factor principle may not actually provide a heightened barrier to access, given that most people use their mobile device as the second factor (you can get the one-time code via text message or from an app installed on the phone).

However, in the case that your laptop is seized, accounts protected by two-factor authentication will not be accessible by the government without the second device that generates the one-time code.

You should revoke trusted-device settings for any accounts that use two-factor authentication before your border crossing to ensure that those accounts ask for the one-time code during the next login attempt.

Full-Disk Encryption

If you need to bring your data with you, the safest way to do so is with full-disk encryption. Full-disk encryption essentially scrambles the contents of your electronic device. The data is unlocked by a passphrase. It also mitigates against the issues with insecure file deletion mentioned above.

Having a strong passphrase for your encrypted data is especially important. A strong passphrase will, in theory, keep your data safe from even the most experienced forensic analyst on the most powerful computers. However, note that it is not clear what would happen if your electronic device is detained and the CBSA is not able to

break your password. Such an approach may result in your device being seized and not returned.

Security experts recommend that you choose a password made up of a series of randomly selected words or a strange phrase. We strongly recommend using a program to randomly generate a passphrase to use for your encrypted disk. If you use a weak password for your encrypted disk, you are taking a risk that it will be cracked.[112]

If you decide to use full-disk encryption, be careful! If you lose your password, your data will be gone forever.

More and more laptop computers are coming with disk encryption software built in.

The Ultimate Editions of Windows Vista and Windows 7 and Windows 10 come with BitLocker, full disk encryption software that can be activated in the Control Panel. Microsoft provides detailed information about the use of BitLocker with Windows 10: https://docs.microsoft.com/en-ca/windows/security/information-protection/bitlocker/bitlocker-overview

Apple computers running OS X 10.7 or later have full-disk encryption built in. You can enable full disk encryption by opening System Preferences, clicking Security, and enabling File Vault. Older Apple computers have File Vault as well, but these versions will only encrypt your user folder. This offers protection for your documents and files stored in that folder, but your applications, system files, and other users' documents will still be accessible.

Up-to-date, modern mobile devices also provide strong encryption. But, older mobile devices and operating systems have known exploits. For example, Elcomsoft, a Russian security company has demonstrated how to break the encryption on Apple's iOS 4 devices.[113]

iPhone devices newer than iPhone 4S *and* iOS 8.3 have strong encryption with no published exploits.[114] However, a commercial forensic vendor claims to be able to unlock even the latest iOS devices.[115]

112 Cory Doctorow, "XKCD on the password paradox: human factors versus computers' brute force", boingboing (10 August 2011), online: <http://boingboing.net/2011/08/10/xkcd-on-the-password-paradox-human-factors-versus-computers-brute-force.html>.

113 ElcomSoft, "ElcomSoft Investigates iPhone Hardware Encryption, Provides Enhanced Forensic Access to Protected User Data" (24 May 2011), online: <https://www.elcomsoft.com/PR/eppb_110524_en.pdf>.

114 Vladimir Katalov, "The art of iOS and iCloud forensics", ElcomSoft blog (2 November 2017), online: <https://blog.elcomsoft.com/2017/11/the-art-of-ios-and-icloud-forensics>.

115 Thomas Fox-Brewster, "The Feds Can Now (Probably) Unlock Every iPhone Model In Existence", Forbes (26 February 2018), online: <https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite>.

Android has allowed full-disk encryption since Android 5, and it is turned on by default since Android 7. However, to take full advantage of full-disk encryption, you need to also turn on the option to require a password upon boot (also called "secure startup").

New Blackberry phones use the Android operating system; they have the same full-disk encryption that is automatically enabled.

Your mobile device may have a separate setting that allows you to encrypt your removable SD card. If you turn this on, you gain the benefits of full-disk encryption, but you will not be able to read the content of the SD card in any other device.

File Encryption

If full-disk encryption isn't for you, you may consider encrypting critical documents or files, especially if those files are privileged or confidential. There are several options for encrypting your files.

Both Mac OS X and Windows have the ability to encrypt files without installing any extra software.

In Windows XP, Vista, 7 or 10, you can create an encrypted folder by right clicking on the folder in Windows Explorer, selecting Properties, selecting the General tab, and clicking Advanced. Select "Encrypt contents to secure data" and click OK. The files in the folder will be visible, but other users will not be able to open or copy those files.

Mac OS X allows you to create an encrypted disk image. Open the Disk Utility application, then press the New button. Enter a name for the disk image, and select a place to save it. Choose a disk size, an encryption type (we recommend 256-bit AES for maximum security), and click create. You will be asked to enter a password. Be sure to pick a strong one, and do not save it to your keychain, or anyone with your login password will be able to access it. Once this is done, you can double click the disk image to open it, then enter your password. It will appear like a disk on your desktop, and any files you put inside it will be encrypted.

Separate Privileged or Confidential Documents

If you have privileged or confidential information on your electronic device, you should at a bare minimum ensure that information is sorted in a way that makes it clear what is and is not privileged.

Privileged information is given the most protection, and in theory should not be viewed by a border officer at all, except to verify that it is what it claims to be (see next section for specific guidance about solicitor-client privilege).

This certainly includes lawyers' files, and can sometimes include doctors' records, psychologists' and psychiatrists' records. Journalists have a limited privilege over their sources.

Many people carry confidential information with them. Accounting records, business records, trade secrets, medical information, academics' research data like transcripts of interviews and survey data, and many other kinds of personal information are considered confidential.

The CBSA is supposed to take precautions not to look at privileged materials when it is warned that those materials exist.[116] However, this is made much more difficult if privileged materials are mixed in with unprivileged materials.

One way to ensure the CBSA is aware of privileged materials is to have separate accounts on your laptop for work and for personal matters. That way, all the privileged information is contained in one user account, which can be pointed out to the officer conducting the search.

Unfortunately, separate accounts are nearly impossible to create with a smartphone without carrying two phones around with you all the time. Keeping separate accounts for your work email and personal email is a good place to start, but even if you take this precaution, it will likely be impossible to completely separate privileged documents from personal documents.

116 CBSA ATI Vol 9, supra note 16 at 39 s 23.6.7.

Solicitor-Client Privilege in the CBSA Context

There is a strong argument that any material over which the client or the lawyer raises a *prima facie* claim of the privilege at the border must not be viewed by CBSA officers at all. Rather, any disclosure of that material must be mediated by a judge who determines the bounds of privilege.

Policy directs CBSA officers to treat documents sensitively if they are protected by solicitor-client privilege. The policy applies to information in "documents, electronic or otherwise" that is communicated between a lawyer and their client for the purpose of providing legal advice.[117] Where there is a suggestion that the documents are subject to privilege, the documents "should be sealed and either returned or sealed in an evidence bag without being examined or read and set aside for review by a court for confirmation of privilege." [118] The policy does not elucidate why or how a CBSA officer would detain an electronic device for such review by a court given that the officer should not be aware of the content of the documents to know whether it has value as evidence of a legal contravention.

The Law Society of British Columbia sought assurance from the government in 2017 that CBSA officers would not seek to search electronic devices by demanding passwords from lawyers. They also sought confirmation that if lawyers refused to provide passwords due to a claim of privilege, that the device would not be seized. The Minister of Public Safety responded by letter advising that CBSA are instructed not to examine information over which privilege is claimed by a lawyer.[119] If you have information that attracts this privilege and plan to cross the border into Canada, you may want to take a copy of this letter to provide to the CBSA officer. Note, however, that the letter is specific to lawyers and notaries, so it is doubtful that legal clients,

117 Canada Border Services Agency, Enforcement Manual Part 4: Examination – Goods and Conveyances, Access to Information Request Previously Released A-2017-10734 (October 2018), at Chapter 3 pg 13, available upon request online: <https://open.canada.ca/en/search/ati/reference/d9028d834c3c6b86cf564e0151842c42>.

118 Ibid.

119 Letter from Ralph Goodale, Minister of Public Safety to Herman Van Ommen, President of the Law Society of British Columbia (28 June 2017), online: <https://www.lawsociety.bc.ca/Website/media/Shared/docs/initiatives/2017RuleofLaw_borderMinisterletter.pdf>.

legal assistants, paralegals or administrative assistants could claim such privilege.

Concern remains, however, that claims of solicitor-client privilege may not be respected by CBSA officers at the border. For example, in a recent court decision, it was revealed by a CBSA officer that "he did not see any limitation on searching a lawyer or judge's phone if they were crossing the border."[120] The Canadian Bar Association has recommended to Canada that a working group be created to collaborate and develop a defined policy for searches at the Canadian border that involve information protected by solicitor-client privilege.[121]

Solicitor-Client Privilege in the Preclearance Context

A claim of solicitor-client privilege over materials on an electronic device will likely not shield them from examination by CBP. The policy says that if solicitor-client privilege is claimed over material on the device, officers are supposed to contact CBP lawyers who will then coordinate with other offices and establish a "Filter Team" to ensure the segregation of any privileged material from other information examined during a search to ensure that any privileged material is "handled appropriately while also ensuring that CBP accomplishes its critical border security mission."[122] There is no clear direction in the policy NOT to search the materials that are under such a claim. In fact, the policy suggests that the CBP are only limited in their search to the extent that they cannot retain copies of materials over which solicitor-client privilege exists unless the materials "indicate an imminent threat to homeland security."[123]

120 R v Gibson, supra note 5 at para 19.

121 Canadian Bar Association, "Privacy of Canadians at Airports and Borders" (Ottawa: September 2017) at 20, online: <https://www.cba.org/CMSPages/GetFile.aspx?guid=04e96564-b5b6-441b-b6de-20b3e0874975>.

122 CBP Search Directive, supra note 98 at para 5.2.1.2.

123 Ibid at para 5.2.1.3.

Best Practices for Interacting with a Border Official

You should not lie to a border officer. Making a false or deceptive statement to a CBSA agent is a criminal offence.[124]

You should not physically interfere with a border officer as they may use physical force in return. Furthermore, hindering a CBSA officer is an offence.[125] You are also required by law to unpack and present any goods you have with you to the officer for inspection.[126] While it is still unclear if this extends to your electronic devices, the border officers may well think it does.

If you have any problems, try to document the names and badge numbers of the officers you interact with at the border. If you decide later to file a complaint about your treatment, knowing the identity of the officer will help.

If your electronic device is seized, politely ask for a receipt (Seizure Receipt K19 or K19RCMP form for a CBSA seizure or a Customs Form 6051D for a preclearance seizure).

If the border officer asks you to unlock your device and you don't want to, politely ask, "do I have to do what you are asking me to, or am I allowed to refuse?" If they give you the option, you could refuse. If there is no option to refuse, communicate clearly that you do not consent to the search and that you are complying under protest, but do not obstruct the officer from carrying out the examination. *The Customs Act* requires passengers to cooperate with officers inspecting their goods when the officer "so requests".[127] Whether this extends to unlocking your device or giving up your password is a gray area, but the officers might well think that it does. Nevertheless, it would be difficult to challenge the legality of a search in a court of law if the officers can show that you voluntarily consented to it.[128]

124 Customs Act, supra note 2, ss 153, 160.

125 Ibid, ss 153.1, 160.1.

126 Ibid, s 13.

127 Ibid, s 13.

128 See e.g. R v Clement, [1996] 2 SCR 289, 1996 CanLII 206 (SCC) for a terse judgment from the Supreme Court ("It is apparent that [the appellant] gave his consent freely and voluntarily. It follows that the search thus consented to did not infringe s. 8 of the Charter." at para 1).

If a border officer insists or orders that you unlock your device, consider the possible outcomes of complying (or not). This is a decision that you should make in light of the particular risks that you face.

The following could happen if you unlock your device for a border officer:

- Border officers can look through any information stored on your device, make a copy of all of it, or seize the device for a lengthy closer look.
- Border officers are not supposed to look at any cloud content that is not located on your device. But if they take your device out of your view, there is no way for you to know.

If you don't unlock your device, the following could happen in the context of a CBSA search:

- Border officers may become suspicious and more interested in searching you, your devices, and your other belongings.
- The officers may take your device and try to access your data on their own, by breaking your password if necessary. This could take a very long time, and you will not have access to your device in the meantime.
- If you are not a Canadian citizen or permanent resident, the border officers can refuse to let you into the country.
- You may be arrested. In 2015 someone was arrested and charged with the criminal offence of "hindering" for refusing to provide his password.[129]
- You may be able to cross the border without any further interference.

129 Josh Dehass, "Man charged for refusing to give border guards his phone password" CTV News (5 March 2017), online: <https://www.ctvnews.ca/canada/man-charged-for-refusing-to-give-border-guards-his-phone-password-1.2266576>.

If you don't unlock your device, the following could happen in the context of a preclearance search:

- Preclearance officers may become suspicious and more interested in searching you, your devices, and your other belongings.
- The officers may take your device and try to access your data on their own, by breaking your password if necessary. This could take a very long time (many months), and you will not have access to your device in the meantime.
- If you are not a US citizen or permanent resident, the preclearance officer can refuse to let you into the country
- You may be flagged for heightened screening whenever you cross the US border in the future.
- You may be able to depart for the US without any further interference.

Recall that in the context of preclearance, you have the right to leave the preclearance area at any stage in the process unless a preclearance officer informs you that they suspect on reasonable grounds that you have committed an offence by either obstructing the officer or by having made a false or deceptive statement.[130]

130 Preclearance Act, supra note 101, s 10(1).

PHOTO CREDIT: OWEN SPENCER

CHAPTER SIX

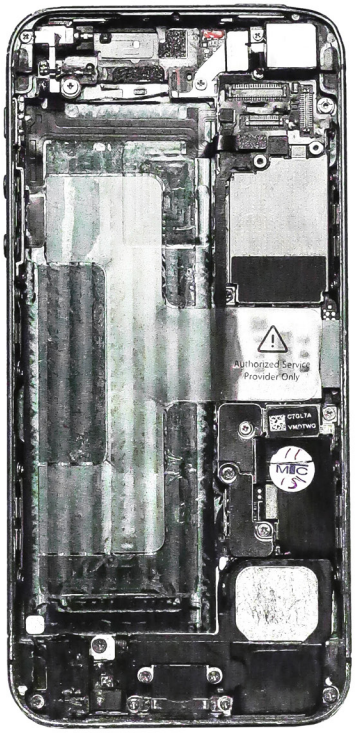
I've Been Searched!

Cleaning Up

If the CBSA or US CBP has plugged any of its hardware into your electronic device, run its software on it, or may have done so while your electronic device was out of your sight, never assume that it is safe to use. The hardware may have also been used on other people's electronic devices. Do you know where those devices have been? It may be possible for the CBSA to accidentally infect you with other people's computer viruses or malware.

We have not seen any evidence to suggest that the CBSA or the US CBP is installing monitoring software on the electronic devices that it searches, but with data security it is better to be safe than sorry. If you suspect that you may be infected with monitoring software, you should not connect it to any of your other devices until making sure it is clean. Software of this type may copy itself to other devices.

First, erase the hard drive entirely or reset the device to the factory settings. This is why making a backup before you travel is absolutely critical. You should also reset the "Master Boot Record" of your computer, which is increasingly



being used to store software that sticks around even after you wipe your system clean.

Once you are back up and running, install and run an antivirus or anti-spyware program on your electronic device. While these programs may not detect the most recent monitoring software, running an antivirus is still an important step to take in reassuring yourself that your electronic device is not passing your data along to third parties.

Calling It In

Once you have made sure that your electronic device is not home to snooping software, you can report the incident.

CBSA Complaint

Unfortunately, the only place to file an official complaint about a CBSA search is to the CBSA itself (unless it is about discrimination or an invasion of privacy). While it is unlikely that your report will have any impact on CBSA policy on its own, if enough people complain, policy might change.

If you would like to contact the CBSA, you have the following options:

If your device or other "goods" has been seized, or you have been issued a penalty or fine, and in a limited number of other circumstances, you can request a review of those actions and decisions with the CBSA. If you disagree with the result of that review, you may also be able to appeal to the Federal Court. For more information, visit: http://www.cbsa-asfc.gc.ca/recourse-recours/howto-commentfaire-eng.html

You can also send your feedback to the Recourse Directorate, which has in the past followed up with complaints about officer conduct. Make sure to include all relevant information so a recourse officer can understands your complaint and can get back to you. The Recourse Directorate can be reached at

Recourse Directorate
Canada Border Services Agency
Ottawa, ON K1A 0L8

The Recourse Program also facilitates the review of external complaints of discrimination filed with the Canadian Human Rights Commission and assists the Department of Justice representing the Agency on appeals to the Federal Court, various tribunals and other external bodies."[131]

Part of the reason so little is known about CBSA policy is because most people who are searched by the CBSA don't talk about it after it happens. We usually only get to hear about searches years after the fact, when a judge issues a decision in a criminal case, for example. We actually know very little about basic things like how many people are searched, what kinds of searches are performed, and what the CBSA is looking for when they do search. This needs to change.

Request Access to your Personal Information that CBSA Retains

The Privacy Act provides people with the general right to gain access to information that is held about them by the CBSA. Visit this website of the Office of the Privacy Commissioner of Canada for details about how to apply for access to your personal information: https://www.priv.gc.ca/en/privacy-topics/access-to-personal-information/accessing-your-personal-information/#fedgov

Office of the Privacy Commissioner

If you feel your personal information has been wrongfully collected, used or disclosed by the CBSA, you may be able to file a complaint with the Office of the Privacy Commissioner of Canada, who oversees the government's compliance with the *Privacy Act.* To find out more, visit https://www.priv.gc.ca/en/report-a-concern/file-a-formal-privacy-complaint/file-a-complaint-about-a-federal-institution/

131 CBSA Report 2016, supra note 38 at 46.

Human Rights Complaint

If you believe that you have been discriminated against by a CBSA officer based on any of the following grounds, you may be able to file a complaint with the Canadian Human Rights Commission:

- race
- national or ethnic origin
- colour
- religion
- age
- sex
- sexual orientation
- gender identity or expression
- marital status
- family status
- disability
- genetic characteristics
- a conviction for which a pardon has been granted or a record suspended

Go to http://www.chrc-ccdp.gc.ca/eng/make-a-complaint to find out how to make a complaint. If you have questions about a potential complaint, the Canadian Human Rights Commission can be contacted by phone at 1-888-214-1090 or at complaint@chrc-ccdp.gc.ca.

Report to Interested Civil Rights Groups

International Civil Liberties Monitoring Group (ICLMG)

The International Civil Liberties Monitoring Group collects reports from people whose rights may have been violated at the Canada or US border. Do you suspect that your name is on a no-fly list or another government watch list? Are you always stopped, searched and interrogated when you attempt to cross the border although you've never been charged or convicted of any crime? Do you believe you have been mistakenly or unfairly targeted? Do you suspect ethnic or religious profiling? Do you no longer travel for fear of being singled out? Travellers who have such experiences when travelling to or from Canada or to the US are encouraged to contact the ICLMG by sending an email to communications@iclmg.ca.

National Council of Canadian Muslims

The National Council of Canadian Muslims (NCCM) is an independent, non-partisan and non-profit organization that protects Canadian human rights and civil liberties, challenges discrimination and Islamophobia, builds mutual understanding, and advocates for the public concerns of Canadian Muslims.

NCCM's Human Rights Department monitors and responds to violations of human rights and civil liberties, and provides dedicated services in challenging discrimination and harassment faced by Muslims in Canada.

If you believe you have been the victim of discrimination or harassment, you can visit the NCCM's website and fill out and submit an Incident Report Form.

Preclearance Complaints

There are a number of avenues to lodge complaints if you think that your privacy has been breached or if you have been discriminated against by CBP officers in preclearance areas.

The Preclearance Consultative Group is comprised of Canadian and US representatives and should be informed of complaints about rights violations in preclearance areas. Currently there is no direct way to file a complaint with this group, but details should be provided prior to the new preclearance law coming into effect. For now, the best contact is Public Safety Canada's Preclearance Unit, part of the International Affairs Division:

Public Safety Canada
International Affairs Division - Preclearance
269 Laurier Avenue West
Ottawa, Ontario K1A 0P8
Canada

Office for Civil Rights and Civil Liberties

The Office for Civil Rights and Civil Liberties at the Department of Homeland Security has a Compliance Branch that investigates complaints alleging discrimination and other civil rights or liberties violations by CBS.

You may file your complaint in a number of ways:

E-mail: CRCLCompliance@hq.dhs.gov (the fastest method to submit your complaint)

Fax: 202-401-4708

U.S. Postal Mail:

U.S. Department of Homeland Security
Office for Civil Rights and Civil Liberties
Compliance Branch
245 Murray Lane, SW
Building 410, Mail Stop #0190
Washington, D.C. 20528

Visit their website for further information.

Chief Privacy Officer

If you think that your privacy has been violated, you may seek redress from the Chief Privacy Officer of the Department of Homeland Security of the U.S. Visit their website for contact information.

Traveller Redress Inquiry Program

The Department of Homeland Security Traveller Redress Inquiry Program (DHS TRIP) is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs - like airports - or crossing U.S. borders. https://www.dhs.gov/dhs-trip.

Report to Interested Civil Rights Groups

Electronic Frontier Foundation (EFF)

The Electronic Frontier Foundation is a leading US nonprofit organization defending civil liberties in the digital world. EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. They work to ensure that rights and freedoms are enhanced and protected as our use of technology grows.

Please direct reports and complaints about border searches by U.S. officials of electronic devices to borders@eff.org.

The American Civil Liberties Union (ACLU)

The ACLU is an organization that promotes and defends civil rights in the U.S. As they monitor civil rights at the US border, they are interested in reports from travellers who think that their rights may have been violated by the US CBP. US residents should report to their local ACLU affiliate while foreigners should report to the ACLU national office. Contact information is available here: https://www.aclu.org/contact-us

Council on American-Islamic Relations (CAIR)

The Washington-based civil rights organization Council on American-Islamic Relations (CAIR) says that there is an unprecedented spike in bigotry targeting Muslims and members of other minority groups since the election of Donald Trump as president. Community members are being urged to report any biased incidents to CAIR by filing a report at: https://www.cair.com/civil-rights/report-an-incident.html

CHAPTER SEVEN

Conclusion

Eventually, the law around border searches will catch up with the way that people are using their electronic devices. Until then, you will have to use the tools at your disposal to maintain your privacy.

The online version of this guide is a work in progress. Check back regularly to find updated information about CBSA and US CBP practices and policies, developments in the law around border searches, and best practices for keeping your data secure.

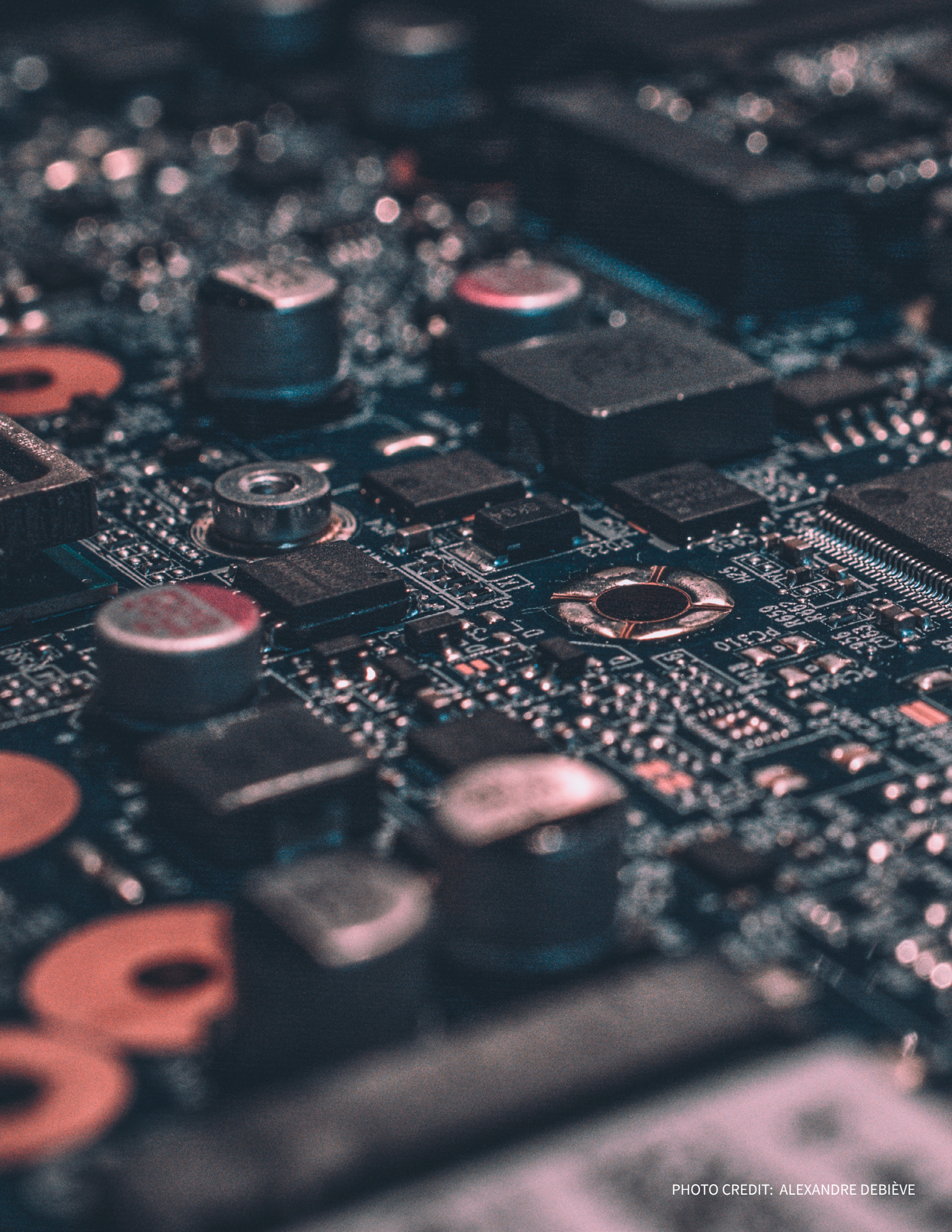


PHOTO CREDIT: ALEXANDRE DEBIÈVE

BC CLA BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

The BC Civil Liberties Association was established in 1962 and is the oldest and most active civil liberties group in Canada. We are funded by the Law Foundation of B.C. and by citizens who believe in what we do.

Our mandate is to preserve, defend, maintain and extend civil liberties and human rights in Canada. We achieve our mandate through our Advocacy in Action, Public Policy, Community Education, and Justice programs.

The BCCLA is an autonomous, non-partisan charitable society. Though we strive to work cooperatively with other groups on common causes, we are unaffiliated with any other organization or political group. Our independence has been one of the BCCLA's enduring strengths for over 50 years.

www.bccla.org

@bccla

@BCCivLib

CIPPIC is the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic at the Centre for Law, Technology and Society, University of Ottawa.

CIPPIC is Canada's first and only public interest technology law clinic. CIPPIC is unique in Canada, bringing together a team of expert legal professionals and students to advocate for the public interest in policy debates arising from the intersection of law and technology. CIPPIC advocates for the public interest on cutting edge issues including copyright law, data governance, algorithmic decision-making, internet governance, net neutrality, state surveillance, privacy and free speech. CIPPIC's work resides at the heart of Canada's innovation policy agenda: CIPPIC ensures respect for Canadians' rights as the law responds to our use of ever-changing technologies.

www.cippic.ca

@cippic