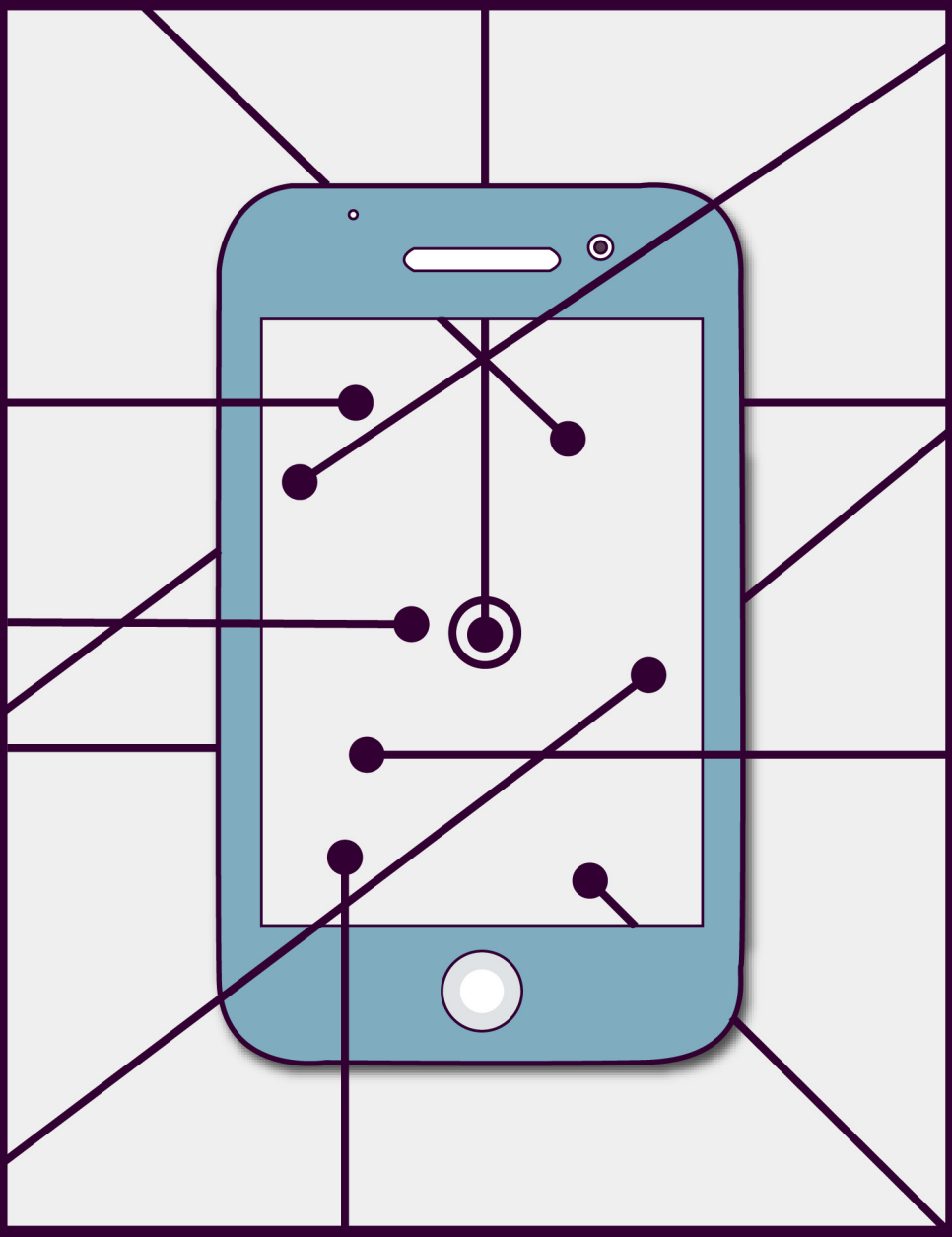
Electronic Devices Privacy Handbook

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.

This project is funded by the Canadian Internet Registration Authority's (CIRA) Community Investment Program.

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 Meghan McDermott (BCCLA), Tamir Israel (CIPPIC), and Greg McMullen, with support from Lex Gill (Citizen Lab), Sancho McCann, Graeme Cook, 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 United States preclearance areas –** What can and can't be done by a preclearance 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 in 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, and can change these at any time, so the information presented here may already be out of date.2 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.

2 Parts of this guide rely on internal CBSA documents that have become public. This includes a 9 volume compendium of documents relating to CBSA 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. This compendium was obtained by the BCCLA through an Access to Information request filed in 2009, and is available on the BCCLA National Security Blog, along with some background regarding the ATIA request: https://bccla.org/2010/05/cbsa-laptop-search-documents/ . Documents within this compendium are referred to throughout this Guide as "CBSA 2009, ATI Volume X" with X being the number of the volume as applicable.

A second compendium of documents was obtained under the ATI Act in 2015 and provided to the BCCLA. This second compendium includes: excerpts from a CBSA customs enforcement manual dated May 8, 2015 and detailing CBSA policies and procedures guiding searches of personal baggage, goods and conveyances (referred to in this Handbook as "CBSA, Customs Enforcement Manual, Personal Goods, May 2015") and a copy of CBSA Operational Bulletin PRG-2015-31, entitled "Examination of Digital Devices and Media at the Port of Entry – Interim Guidelines", June 30, 2015. This compendium of documents is available on the BCCLA website: https://bccla.org/wp-content/uploads/2016/08/CBSA-FOI-Docs.pdf.

The final version of the Interim Guidelines issued in CBSA Operational Bulleting PRG-2015-31 was provided by the CBSA to the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) in 2017, and is appended to ETHI's subsequent report: ETHI, "Protecting Canadians' Privacy at the US Border", December 2017, Appendix A: "Operational Bulleting PRG-2015-31, Examination of Digital Devices and Media at the Port of Entry – Guidelines", Issued: June 30, 2015, updated February 28, 2017, http://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9264624/ethirp10/ethirp10-e.pdf. These Guidelines appear to have been in force since June 2015 and to be current as of February 2017. They are referred to throughout this guide as: "CBSA Operational Bulletin, PRG-2015-31".

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 people do not expect to be able to cross international borders free from scrutiny, meaning the CBSA has more power to carry out searches for the purpose of ensuring only lawful goods and people enter the country. As a result, privacy protections at the border fall along a spectrum. While a police officer could not stop someone in the street and randomly search their bag, routine searches of people and goods are allowed at the border with minimal limitation. As searches become more invasive, more safeguards and restrictions apply.

Locating border searches of electronic devices along this spectrum of safeguards is an evolving process. CBSA practices and Canadian courts are increasingly aware of the unique concerns that electronic devices pose for privacy, even at the border. However, judges continue to uphold random border searches of electronic devices 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* prevents some goods from being imported into Canada and places conditions such as customs fees on others. It gives the CBSA broad powers to search both people and goods coming into the country for this purpose.[3]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.[4] 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 privacy rights that we enjoy within Canada's borders do not directly extend to the border.

The *Customs Act* makes it clear that border officers' ability to search goods includes "any document in any form."[5]

Canadian courts have found that electronic devices as well as the files that are stored on them count as goods under the Customs Act, and that the CBSA has the power to search these in the same way as they could search any other goods and documents.[6]

Early CBSA documents show that it treated computer files the same way it would treat a briefcase full of documents, claiming that "the only difference between a paper document and information stored electronically is the medium it is stored on."[7] More recent CBSA policies, current as of 2017, indicate a cautious approach to searches of electronic devices out

3 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). See also R v Simmons, [1988] 2 SCR 495, paras 48-49.

4 R v Simmons, [1988] 2 SCR 495, para 49: "travellers seeking to cross national boundaries fully expect to be subject to a screening process."

5 Customs Act, supra note 3.

6 See, e.g., R. v. Saikaley, 2012 ONSC 6794 at para 102 ("the Applicant's iPhone ... is included in the definition of 'goods'"); R. v. Buss, 2014 BCPC 16 at para 25 ("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"); R. v. Moroz, 2012 ONSC 5642 at para 20 ("the expression 'goods' ... reflect[s] the type of information found in electronic devices such as a cell-phone or an I-Phone."); R. v. Whittaker, 2010 NBPC 32 at para 8 ("[A] computer file such as the digital storage of photographic images is a document and falls squarely within the definition of 'goods'"); R. v. Appleton, [2011] 97 WCB 2(d) 444 at para 12 (Ont SCJ) ("The texts may not be goods in themselves, but could be located while on a search for goods."); R v Gibson, 2017 BCPC 237, (data on a digital device counts is a 'good' but data not already on the device at time of border crossing such as an email that has not been downloaded is not).

7 CBSA 2009, ATI Volume 2, p 5. At pp 9-10, CBSA ATI Volume 2 explains in more detail: "Text and images are often contained in laptops, cell phones, memory stickes or other electronic devices ... Within the normal customs process, these items can be examined. The examination is more a scan for indicators." See footnote 4 for more details.

of recognition that such "examinations are usually more personal in nature than baggage examinations" and might therefore attract more stringent *Charter* protections.[8] However, the CBSA continues to maintain its right to conduct random searches of devices for customs purposes.[9]

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 failed.[10]

Under the *Customs Act*, the CBSA may also seize a device under certain conditions.[11] This should not occur on a random basis, but only where the CBSA has sufficient grounds to believe that the device in question contains contraband such as child pornography or evidence of a contravention of the Customs Act.[12] However, the CBSA will not necessarily tell you their rationale for taking your device.

The Immigration and Refugee Protection Act

The *Immigration and Refugee Protection* Act governs immigration to Canada. It grants the CBSA powers to search people and their personal effects to determine their identity and admissibility into Canada.

Under this statute, a CBSA officer may search the "luggage and personal effects" of a person seeking to come to Canada without a warrant.[13] Such searches cannot be carried out randomly and without suspicion of wrongdoing, but only where an officer has reasonable grounds to believe that the person has not revealed their identity or has hidden, on or about

8 CBSA Operational Bulletin, PRG-2015-31, p 4.

9 Ibid , p 1: "Paragraph 99(1)(a) of the Customs Act provides CBSA officers with the legislative authority to examine goods, including digital devices and media, for customs purposes only. Although there is no defined threshold for grounds to examine such devices, CBSA's current policy is that such examinations should not be conducted as a matter of routine; they may only be conducted if there is a multiplicity of indicators that evidence of contraventions may be found on the digital device or media."

10 R v Leask, 2008 ONCJ 25 at 100; R v McDermin, 2008 CanLII 68135 (Ont SCJ); R v Whittaker (2010), 946 APR 334 (NBPC), R. v. Gibson, 2017 BCPC 237. By contrast, however, see United States of America v Amadi, 2017 ONSC 3446, para 50: "The search powers of border agents … have not been considered by the courts since the release of the judgment of the Supreme Court of Canada in R v Fearon. While there is undoubtedly a reduced expectation of privacy upon crossing a border, there is also a reduced expectation of privacy upon arrest as articulated in Fearon. This does not mean that the power to search is limitless. The proposed argument that there are limits to the power to search electronic devices at the border has an air of reality." See also: R v Vaillancourt, 2017 MBQB 95, paras 3 and 8.

11 Customs Act, supra note 3, ss 110(1) – (3).

12 R v Gibson, 2017 BCPC 237, paras 47 and 188.

13 Immigration and Refugee Protection Act, SC 2001, c 27, https://www.canlii.org/en/ca/laws/stat/sc-2001-c-27/133506/sc-2001-c-27.html at s 139(1).

their person, documents that are relevant to their admissibility.[14] A CBSA officer may also search the "luggage and personal effects" of a person seeking entry in to Canada if there are reasonable grounds to believe that the search will reveal documents that could be used in certain immigration offences: people smuggling, human trafficking or immigration-related document fraud. [15]

A CBSA Operational Bulletin current to 2017 makes it clear that "digital devices and media" are interpreted as "personal effects" and thus searchable under these powers.[16] Searches of devices and media should be limited to identifying the person, finding documents related to their admissibility into Canada, and finding evidence of crimes related to entry into Canada.[17]

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. This is due to the protection against unreasonable search and seizure that is provided by the Charter.[18]

This is not the case during a border crossing.

At the border, the CBSA can search anything carried by a person and any imported goods without suspicion. In the past, this has included brief patdowns of a travelers' clothing,[19] detailed searches of luggage,[20] or reading a traveller's bankbook.[21]

14 Ibid at s 139(1)(a).

15 Ibid at s 139(1)(b): authorizes searches where there are reasonable grounds to believe a person has committed, or possesses documents that may be used in the commission of, an offence referred to in section 117 (people smuggling), 118 (human trafficking) or 122 (possession or use of documents for the purpose of contravening the Act).

16 CBSA Operational Bulletin, PRG-2015-31, supra note 2.

17 Ibid.

18 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.

19 R v Simmons, supra note 4 at para 27.

20 CBSA, Customs Enforcement Manual, supra note 2, Part 4, Chapter 3, May 8, 2015, paragraph 37: "Officers may use contraband detection equipment and tools, including detector dog teams, to assist them in the examination of personal baggage…when deemed appropriate. NOTE: The use of contraband detection equipment such as inspection mirrors and flashlights, fibrescopes, probes, x-ray systems may assist in the examination of visually limited areas of vehicles or luggage."

21 R v Jones, [1992] BCJ No 231 (BCSC).

Even a suspicionless search must be generally related to the objective that justifies it. In the CBSA context, a random search can only be carried out for the purpose of regulating what goods individuals bring into Canada and the CBSA requires a "clear nexus" to a customs objective of this sort.[22] A CBSA officer could not, for example, search their neighbour's mobile device to uncover local gossip—even at the border.[23] Additionally, random searches should not be motivated by racial profiling, meaning that the CBSA should not single you out for search based on markers such as race, gender or religion.[24] Finally, searches that are intended to further a general criminal investigation are not an 'examination of goods' within the context of the *Customs Act* and should not be conducted on a random basis.[25] In practice, however, random customs searches can be justified by many innocuous factors and it is difficult to identify situation where an individual's electronic device is singled out to be searched on the basis of personal concerns, racial profiling or general criminal investigation.[26]

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 digital devices without a warrant or even suspicion, there are limits to those searches.

A CBSA document indicates 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.[27] The

22 CBSA Operational Bulletin, PRG-2015-31, supra note 2 at p 1.

23 R v Gibson, supra note 12 at paras 181-184: "the search must be conducted for a valid customs purpose."; R v Appleton, [2011] 97 WCB (2d) 444, para 12; United States of America v Almadi, 2017 ONSC 3446, paras 48-49 and 51. CBSA policies similarly note that "Examinations of digital devices and media must always be performed with a clear nexus to administering or enforcing CBSA-mandated program legislation that governs the cross-border movement of people and goods..." (CBSA, PRG-2015-31, supra note 2).

24 R v Simpson, 2017 ONSC 491; R v Smith, [2004] 26 CR (6th) 375 (ONSC), paras 29 and 34.

25 R v Jacoy, [1988] 2 SCR 548; R v Gibson, 2017 BCPC 237; R v Appleton, [2011] 97 WCB (2d) 444 (ONSC), para 12; United States of America v Almadi, 2017 ONSC 3446, para 49 (a search of a phone that is in furtherance of a criminal investigation is not an 'examination of goods' and therefore not justified under the Customs Act's random search provisions).

26 R v Simpson, 2017 ONSC 491, paras 30 and 52; R v Moroz, 2012 ONSC 5642, paras 3-5 and 17: (police who do not have enough grounds to obtain a search warrant may issue a 'Lookout' to the CBSA if they know their suspect intends to travel. If the CBSA acts on this 'Lookout' when singling out the suspect's goods and electronic devices for a search upon her or his re-entry into Canada, the search remains an 'examination of goods' and can be conducted randomly under the Customs Act).

27 CBSA ATI Volume 9, supra note 2 at p 36-37.

CBSA operates under a policy, current until at least 2017, which indicates that electronic devices should not be conducted routinely, but only where a "multiplicity of indicators" suggest the search will yield evidence related to a customs enforcement goal.[28]

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 digital device.[29] Officers can only look 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.[30] 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 the CBSA finds things on your electronic device that leads it to believe that you may have contraband, they may order 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. A CBSA policy states that officers should not only have a reason for carrying out more detailed searches of electronic devices, but should make a note of what led them to search specific areas of your device beyond the initial cursory search.[31] However, CBSA officers will not necessarily tell you the reasons for their progressively more invasive searches.

28 CBSA Operational Bulletin, PRG-2015-31, supra note 2.

29 CBSA ATI Volume 4, supra note 2, p 10 at s 42.

30 R v Hardy (1995), 103 CCC (3d) 289 (BCCA), paras 32 and 61; R v Sekhon, 2009 BCCA 187 at para 91. Current CBSA policies also reflect this approach: CBSA, Customs Enforcement Manual, Part 4, Chapter 3, May 8, 2015, para 76: "Officers must have reasonable grounds and must be able to clearly articulate such grounds before cutting, drilling and/or dismantling [of personal baggage] is undertaken during an examination." Different considerations might apply with respect to commercial / non-personal luggage or containers: R v Lapple, 2016 ONCA 289, paras 6-11.

31 CBSA Operational Bulletin, PRG-2015-31, supra note 2: "Examination Progression".

Accessing Remote Content & Social Media Activity

Your phone is not only a container for many of your most intimate photos, discussions and interactions, but also a portal to a range of remote content including your social media accounts, your health monitoring tools, your car or even your smart refrigerator.

The CBSA's authority to access these types of accounts when searching your phone is on less firm footing than its ability to search data already on the device such as photos you have taken, your list of phone contacts, data backups you have stored on the cloud, or emails and text messages you have received.

As explained above, the CBSA has wide powers to randomly search 'goods' being imported into Canada and courts have held that this includes electronic devices and the data stored on them. However, some courts have held that any data which has not already been downloaded unto your phone or laptop when you are crossing the border falls outside this definition.[32] Known CBSA policies reflect this distinction, noting that officers "shall only examine what is stored within the device" and shall not read remote content that has not yet been downloaded and read by the device owner.[33] However, the CBSA has been known to ask a traveller to voluntarily log in to a remote account.[34]

If consistently applied, this policy should prevent CBSA officers from accessing live social media content through accounts linked to a device that's being searched. However, as there is no clear statement on this matter to date, travellers should not expect their linked social media accounts to remain private when crossing the border. In addition, travellers should be aware that much social media activity is public, and the CBSA has been known to proactively monitor the activity of Canadian and foreign travellers destined for the Canadian border.[35]

32 R v Gibson, supra note 12 at paras 95-96: "data imported on an electronic device … is restricted to data that is stored on the electronic device at the time it is being imported. When the electronic device is being searched by the Customs officer, in order to comply with the Customs Act, it should be placed in a mode that does not permit it to access the internet. For greater certainty, that means that data stored on the cloud, on remote networks, or remotely on other devices not in the possession of the traveller at the time they are crossing the border, and not stored on the device(s) in their possession at the time they cross the border, is not searchable at the instance by the BSO. Data stored remotely is not a good being imported by the traveller at the time they present themselves to the BSO pursuant to s. 12(1) of the Act, nor is it a good that has been imported pursuant to s. 99(1)(a). However, hard drives, USB sticks and other data storage devices in the actual possession of the traveller or in their possession in their accompanying baggage at the time they present themselves at the Customs office is a good, and subject to inspection."

33 CBSA Operational Bulletin, PRG-2015-31, supra note 2: "CBSA officers shall disable wireless and Internet connectivity (i.e. set to airplane mode) to limit the ability of the device to connect to remote hosts or services … [and] shall only examine what is stored within the device. Officers are not to read emails on digital devices and media unless the information is already downloaded and has been opened (usually marked as read)."

34 Ward v Canada (Minister of Public Safety and Emergency Preparedness), 2014 FC 568.

35 For example, prospective air travellers are identified for social media monitoring on the basis of scenario-based risk assessment algorithms, Office of the Privacy Commissioner of Canada, Canada Border Services Agency – Scenario Based Targeting of Travelers, Audit Report, September 21, 2017, https://www.priv.gc.ca/en/opc-actions-and-decisions/audits/, paras 8 and 16-17.

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.

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 digital devices is still limited, some CBSA documents have become public in recent years, shedding some light on the subject. These documents provide some information on how the CBSA chooses people to search, how those searches *should* be done, and what happens to the data they collect.[36] Included in these documents is a 2015 CBSA Operational Bulletin governing its examination of digital devices and media at ports of entry, which is confirmed to be current as of 2017.[37]

Please note that guidelines, policies, bulletins, manuals and other kinds of documents used by the CBSA *do not have the force of law*. Although these documents may appear to the public as binding rules, the CBSA is not necessarily obligated to follow these policies and might change them at any time.

No Access to Remote Data

The CBSA has no authority under the *Customs Act* to search data that is not already on an electronic device.[38] 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 or otherwise connect their device to the Internet. If the CBSA wants to search information that is only accessible once a device is connected to the cloud, the agency claims it will typically obtain a warrant issued by a judge. [39]

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.[40] Officers should set the device to airplane mode prior to searching to "reduce the possibility of triggering remote

36 *Supra* note 2.

37 CBSA Operational Bulletin, PRG-2015-31, supra note 2.

38 R v Gibson, supra note 12 at para 92.

39 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].

40 R v Gibson, supra note 12 at para 92.

wiping software, inadvertently accessing the Internet or other data stored externally or changing number versions or dates."[41] 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.[42] 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."[43]

The agency maintains that it has the authority under the *Customs Act* to search electronic devices without suspicion.[44] 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, and should "not be conducted as a matter of routine."[45] CBSA officers are also directed not to examine electronic devices "with the sole and primary purpose of looking for evidence of a criminal offence under any Act of Parliament."[46]

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

41 CBSA Operational Bulletin, PRG-2015-31, supra note 2 at 25.

42 *Ibid.*

43 *Ibid.*

44 *Ibid* at 23.

45 *Ibid* at 24.

46 *Ibid.*

is a multiplicity of indicators that evidence of contraventions may be found" on the device.[47] 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.[48]

If the CBSA officer sees something that they feel needs a closer inspection, a slightly more thorough search can 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 should only progress if new indicators emerge or there is a discovery of undeclared, prohibited, or falsely reported goods or of immigration-related offences such as document or identity fraud.[49]

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.[50] The officers must be able to explain how they expect each document, application, or program they examine to be relevant to verifying their concerns.[51] However, they are not obligated to provide you with this explanation.

CBSA officers may look for obscenity, child pornography or hate literature on devices and media, as well as evidence of contraband. However, the CBSA does not have the best track record with distinguishing between legal and illegal pornography, and has been known to seize pornography that is completely legal.[52]

Sometimes, CBSA officers might 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

47 *Ibid* at 23.

48 CBSA ATI Vol 9, *supra* note 2 at slide 5.

49 CBSA Operational Bulletin, PRG-2015-31, *supra* note 2.

50 *Ibid* at 25.

51 *Ibid.*

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

she was coming to Vancouver to give before the 2010 Winter Olympics. As a part of her examination, the CBSA searched her electronic device.[53]

Where a CBSA officer uncovers evidence of a criminal offence while conducting a search of an electronic device or other electronic media, that officer must "be cognizant of where the regulatory [that is, customs-related] 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.[54]

When the officer's concern is conclusively resolved, like when someone proves that they are a Canadian citizen and may enter the country as of right, the officer may not continue going through the documents.[55]

53 "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>.

54 CBSA Operational Bulletin, PRG-2015-31, *supra* note 2 at 24-25.

55 CBSA 2009 ATI Volume 1, *supra* note 2 at 6.

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 of electronic devices. 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 BCCLA has 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 or 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 to 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.[56]

Taking disc images also allows the CBSA to run password-cracking software to try and access any data on the device that 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. In addition, many devices include mechanisms that prevent too many passwords from being guessed incorrectly over a short period of time.

Tips on picking a strong password are below, in Section 4 – Best Practices.

56 CBSA ATI Vol 9, *supra* note 2 at 36-37.

Where a device is not encrypted, the CBSA will be able to access data stored on it even without knowing or guessing any passwords put in place to protect the data. This is because data can often be copied directly from an unencrypted device even without entering its password, and that data can then be searched using forensic software. Applications or data that are independently encrypted will continue to pose a challenge in terms of access regardless of whether the device itself is encrypted. However, even where a device or data on it is encrypted, the CBSA might be able to access its contents without knowing or guessing the password by using third party tools that exploit security vulnerabilities.[57]

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

57 Lex Gill, Tamir Israel & Christopher Parsons, "Shining a Light on the Encryption Debate: A Canadian Field Guide", May 2018, CIPPIC / The Citizen Lab, https://cippic.ca/uploads/20180514-shining_a_light.pdf, pp 81-84.

Suspicionless Searches

In theory, random or suspicionless 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.

Targeted Searches

Most of the people searched by the CBSA are not chosen at random, but rather through various pre-arrival targeting mechanisms such as 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.[58] The program uses methodologies that are aligned with the United States. Being identified by the program might lead to more intrusive border searches of electronic devices.

The information about a person that is analyzed includes the Advance Passenger Information (API) and Passenger Name Record (PNR) data that all commercial entities carrying persons or goods into Canada by air are required to send to CBSA under law.[59] 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.[60] The PNR

58 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].

59 *Passenger Information (Customs) Regulation*, SOR/2013-219, April 24, 2018, https://www.cbsa-asfc.gc.ca/publications/dm-md/d1/d1-16-3-eng.pdf.

60 Canada Border Services Agency, "Guidelines for the Access To, Use and Disclosure of Advance Passenger Information (API) and Passenger Name Record (PNR) Data, Memorandum D1-16-3, April 24, 2018, https://www.cbsa-asfc.gc.ca/publications/dm-md/d1/d1-16-3-eng.pdf, p 1.

information may include ticketing information, baggage information, address, contact phone numbers, seat number and payment information.

This information is uploaded to the Passenger Information System (PAXIS) where it is retained for 3.5 years or, to the extent required for an ongoing investigation, up to 6 years.[61] The CBSA conducts multi-faceted and multi-dimensional risk assessments of this and other pre-arrival information in order to identify people and goods that might require closer scrutiny upon arrival at a port of entry into Canada.[62]

With respect to air travellers in particular, one targeting method involves the use of algorithms to match individuals against scenarios for automated risk assessment.[63] Scenarios are used to assess air travellers for what are considered predictive risk factors in areas such as immigration fraud, smuggling of contraband, terrorism and organized crime.[64] These scenarios are not publicly available, for security reasons.[65]

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 United States border authorities. The NTC officer may also search national and international databases, a review of tax records and social media.[66] 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.[67] Targeted travellers will be subject to questioning and possibly further examination by CBSA once they arrive at the Canadian Port of Entry.

---

61 *Protection of Passenger Information Regulations*, SOR/2005-346, last amended March 11, 2016, http://laws.justice.gc.ca/PDF/SOR-2005-346.pdf, s 3.

62 Canada Border Services Agency, "Evaluation of the Canada Border Services Agency Targeting Program", *CBSA Internal Audit and Evaluation Directorate*, January 2016, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/ae-ve/2016/tp-pc-eng.html. See also: Canada Border Services Agency, "Audit of National Targeting", December 2015, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/ae-ve/2015/nt-cn-eng.html, Diagram 2: "Simplified Targeting Process Illustrating Inputs" and Canada Border Services, "Evaluation of Traveller Processing (Marine)", *CBSA Internal Audit and Program Evaluation Directorate*, May 2017, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/ae-ve/2017/tpm-tvmm-eng.html.

63 *Customs Act*, *supra* note 3, s 107(3) and *Immigration and Refugee Protection Act*, *supra* note 13, s 149(a) authorize the use of passenger information for this purpose.

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

65 *Ibid,* at para 8,.

66 *Ibid*, at paras 6-8 and 20.

67 *Ibid,* at para 7.

Of the 29 million travellers who arrived in Canada by commercial air carrier in 2016-17, approximately 60,000 (0.2%) of travellers were flagged under the SBT for national security purposes alone. [68] Of these, 552 travellers were identified for further examination upon arrival in Canada. This represents 0.002% of travellers in that calendar year. [69]

Other Databases & Pre-Arrival Targeting Mechanisms

In addition to the National Targeting Program, individual travellers might be identified for closer scrutiny at ports of entry through the application of a range of other pre-assessment tools.

The CBSA operates a system of 'Lookouts' that identify specific persons, corporations, conveyances or shipments for closer scrutiny and possible exclusion or even arrest at Canadian ports of entry.[70] These lookouts can be entered into the CBSA's system at the agencies' own initiative, at the request of another Canadian agency, or at the request of a foreign agency.[71] Lookouts are available to frontline CBSA officers and an individual who is the object of a Lookout will be subjected to more intrusive searches when seeking to enter Canada.[72] At times, a Canadian agency such as the RCMP might use this mechanism in order to encourage the CBSA to search an individual suspect that the RCMP lacks sufficient grounds to search within Canada.[73] Lookouts are currently issued and acted upon even under circumstances where requesting agencies such as the RCMP would have no legal grounds to search an individual or their devices within Canada.[74] While these practices risk transforming the border security context into what is essentially a domestic

68 *Ibid,* between paras. 30 and 31 (CBSA response).

69 *Ibid,* between paras. 30 and 31 (CBSA response).

70 Canada Border Services Agency, Audit of Lookouts – Traveller Mode, June 2013, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/ae-ve/2013/altm-asmv-eng.pdf, p 3.

71 Audit of Lookouts, *ibid*, at 3-4 and footnote 3.

72 Canada Border Services Agency, Report on Plans and Priorities 2016-17, https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/rpp/2016-2017/rpp-2016-2017-eng.pdf, p 20: "A lookout 'hit' requires a mandatory referral to a secondary examination."; See also: *R v Moroz*, 2012 ONSC 5642, para 5.

73 *R v Moroz*, 2012 ONSC 5642, paras 3-7; *R v Saikaley*, 2017 ONCA 374, leave to appeal ref'd, [2017] SCCA No 284. However, the constitutionality of this practice has not yet been definitively assessed by the courts (see para 60).

74 *R v Moroz*, 2012 ONSC 5642, paras 3-7; *R v Saikaley*, 2012 ONSC 6794, paras 83-89; *R v Saikaley*, 2017 ONCA 374, leave to appeal ref'd, [2017] SCCA No 284.

law enforcement tool, courts to date have not censured the practice.[75]

The CBSA also relies to a range of other databases and pre-arrival assessment mechanisms. For example, TIPOFF US/Canada (referred to as 'TUSCAN') is a US-controlled list of individuals flagged as potential national security suspects and used by the CBSA in deciding whether an individual should be subjected to closer scrutiny, denied entry or arrested at a point of entry.[76] In addition, CBSA officers have access to Canadian Police Information Centre (CPIC), a national database that records interactions between law enforcement and individuals.[77] All of this pre-arrival profiling and information-gathering can be relied upon by CBSA officers when deciding whether to search an individual's device at the border.

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."[78] 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.[79]

75 *Ibid.*

76 Online: http://www.documentcloud.org/documents/4573306-Public-Safety-Canada-TIPOFF-U-S-CANADA-TUSCAN-a.html

77 Information and Privacy Commissioner of Ontario, "Crossing the Line: The Indiscriminate Disclosure of Attempted Suicide Information to US Border Officials via CPIC" (April 14, 2014), online: https://www.ipc.on.ca/wp-content/uploads/Resources/indiscriminate_disclosure.pdf.

78 *R v Canfield,* 2017 ABQB 350 at para 42.

79 *Ibid,* at para 46.

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

- Are importing something the CBSA deems to be suspicious.[80] 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".[81]
- Have travelled to and from "high risk" destinations.[82] 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[83] and Spain.
- Are a single man traveling alone.[84]
- Demonstrate "an interest in Pornography".[85] 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.[86]
- Exhibit nervousness, agitation, are talking fast, contradicting oneself.[87]
- Have multiple electronic devices (including hard drives).[88]
- Purchase a ticket to travel as the last minute, within days of departing for the trip.[89]
- Are hesitant in answering questions or being flagged on a database.[90]
- Have coding on your suitcase that doesn't match where you are coming from.[91]
- Have "unusual" travel routes (e.g. travelling to Canada from Illinois by car but only crossing the border in Vancouver).[92]

Finally, the discovery of an electronic file named "porno" in one case was an indicator that the CBSA determined required further inspection and a more progressive search.[93]

80 CBSA ATI Vol 4, supra note 2 at 6 s 32.

81 CBSA ATI Vol 6, *supra* note 2 at 13.

82 CBSA ATI Vol 4, *supra* note 2 at 6 s 32.

83 *R v Canfield, supra* note 78 at para 56.

84 "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/>.

85 CBSA ATI Vol 9, *supra* note 2 at 3 slide 9.

86 CBSA ATI Vol 4, *supra* note 2 at 6 s 32.

87 *R v Canfield,* supra note 78 at paras 35 and 53.

88 *Ibid,* note 44 at para 53.

89 *Ibid,* note 44 at para 56.

90 *R v Buss, supra* note 3 at para 12.

91 ETHI Evidence, *supra* note 22.

92 *R v Gibson, supra* note 12 at para 7.

93 *R v Mozo,* 2010 Carswell 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.[94]

Initial data from the CBSA about such examinations has been made available through an access to information request.[95] The information is limited to a period of 16 weeks and indicates that about 40 electronic devices, on average, are "examined" each day.[96] Of these devices that are examined, an average of 13 are "searched."[97] 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.[98]

Passwords

If your electronic devices are searched, the CBSA will ask you to provide any passwords required to access the information on them.[99] Sometimes a password is required to unlock the device itself. Other passwords may be required to

94 ETHI Evidence, supra note 22.

95 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/040b79163c-96b8a8b52579f91015806f>.

96 *Ibid.*

97 *Ibid.*

98 *Ibid.*

99 CBSA ATI Vol 9, supra note 2 at 3 slide 9.

open specific software or "apps" on the device or to access specific content on the device.

Am I Obligated to Provide Passwords to My Devices and Data?

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 and what the consequences of refusing might be. 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." [100] A CBSA officer also has the power to arrest a person at the border for "hindering"[101] or "obstructing"[102] an officer in the performance of their duties.

In general, it is not permitted to hinder or prevent a border officer from doing anything that officer is authorized to do under the *Customs Act*. Refusing to unlock the trunk of a car or a glove box might therefore amount to 'hindering' or 'preventing' a border officer from carrying out his or her authorized search of a car.[103] However, if the refusal in question does not actually prevent the CBSA officer from carrying out their search, then no crime has occurred. For example, in one case, an individual refused to provide a border official with his wallet upon demand. However, since the border official could legally take the wallet physically from the individual's back pocket, refusing to provide the wallet did not amount to 'hindering'.[104] Had the individual traveller physically prevented the border official from taking the wallet, however, he might have been successfully tried with hindering.[105] This general framework applies to passwords if lack of a password prevents a border official from accessing an electronic device.

The issue is muddled because the question has yet to be directly considered by a courts. Legal scholars have objected to mandatory password disclosure at the border. Some have argued that while devices and data that accompany travellers as they leave and re-enter Canada are difficult to classify as 'goods being imported

100 *Customs Act, supra* note 3, s 13.

101 *Customs Act, supra* note 3, s 153.1.

102 Immigration and Refugee Protection Act, supra note 8, s 129(1)(d).

103 R v Cimini, [2008] OJ No 5380 (ONCJ), para 18.

104 Ibid.

105 Ibid.

into Canada'. It is therefore difficult to argue that refusing to provide a password to such devices and data might be considered 'hindering a search for imported goods.[106] Others have argued that searches of electronic devices and data are unlikely to actually yield contraband, and border device searches are fundamentally more a means of obtaining back door access to private information that could not be otherwise obtained by domestic law enforcement and other agencies and hence should not be granted the same latitude as other customs-related border searches.[107] Still others have argued that device searches are highly intrusive in nature and as such the CBSA can only carry these out while respecting the full range of constitutional safeguards. This includes rights such as the right to consult a lawyer, the right to remain silent and the right not to be forced to participate in an investigation of your own alleged criminal conduct, which prevent law enforcement agencies from forcing password disclosure in non-border contexts.[108]

Another question arises where a device or application is protected by a password, but is not encrypted. If border officials are able to access this data without the password using frontline forensic tools, then refusing to provide your password might not amount to 'hindering' or 'preventing' a border official carrying out an authorized search.[109]

However, courts have yet to endorse these approaches. Indeed, in one case, 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.[110] In another case, a court noted in passing that a person is subject to arrest if they don't reveal their password.[111] There is also one known case in which the CBSA arrested a traveler when he failed to reveal his e-device password, and the individual in question eventually plead

106 Robert J. Currie, *Electronic Devices at the Border: The Next Frontier of Canadian Search and Seizure Law?* (2016) 14 Can. J. L. & Tech. 289.

107 Steven Penney, "'Mere Evidence'? Why Customs Searches of Digital Devices Violate Section 8 of the *Charter*", (2016) 49(1) *UBC L Rev* 485.

108 Lex Gill, Tamir Israel & Christopher Parsons, "Shining a Light on the Encryption Debate: A Canadian Field Guide", May 2018, *CIPPIC / The Citizen Lab*, https://cippic.ca/uploads/20180514-shining_a_light.pdf, pp 72-76; *R v Boudreau-Fountaine*, 2010 QCCA 1108; *Re: Impression Warrant Application (s 487.092)*, 2016 ONCJ 197; *R v Boutros*, 2018 ONCA 375, paras 12-14 & 27; *R v Talbot*, 2017 ONCJ 814.

109 *R v Cimini*, *supra*.

110 *R. v. Whittaker*, 2010 NBPC 32 at para 4.

111 *R v Canfield*, *supra* note 78 at para 44.

guilty to hindering, accepting a fine of $500.[112] CBSA "Interim" guidelines that were in effect from mid-June 2015 until an unknown recent date directed officers to temporarily refrain from arresting individuals on the sole basis that they have refused to provide a password to their device upon demand.[113] 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." [114] The current and finalized version of this policy, however, removed this restriction and 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.[115]

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 an officer has the authority to compel a traveler to provide it 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 e-device.[116] In most cases, people at the border cooperate and provide a password, although it is not clear whether this occurs because people are voluntarily cooperating or because believe they are obligated to do so.[117] 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." [118]

What is clear is that CBSA officers may only demand passwords required to gain access to e-devices or other electronic media, or files that are known or suspected to exist within these. CBSA officers may not compel passwords to gain

112 Brett Ruskin, "Alain Philippon Pleads Guilty Over Smartphone Password Border Dispute", *CBC News*, August 15, 2016 http://www.cbc.ca/news/canada/nova-scotia/alain-philippon-to-plead-guilty-cellphone-1.3721110.

113 CBSA, PRG-2015-31, INTERIM, issued June 30, 2015, p 4: "Until further instructions are issued, CBSA officers shall not arrest a traveller for hindering … or for obstruction … solely for refusing to provide a password."

114 CBSA 2015 ATI, *supra* note 2 at 5.

115 CBSA, PRG-2015-31, FINAL, updated February 28, 2017, *supra* note 2.

116 Bolduc testimony http://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-69/evidence#Int-9671565

117 To date, courts have held that no rights are engaged where an individual is asked at the border to provide a password and voluntarily complies.

118 Bolduc testimony http://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-69/evidence#Int-9671565

access to any account, file or information that might potentially be stored remotely or online.[119]

What to Expect If You Provide Password(s)

If you do give your password to the CBSA, you will not be permitted to input it yourself unless the device is biometrically protected (i.e. fingerprint).[120] 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.[121]

With non-biometric passwords, CBSA officers are to request the password to access the device and to record the password and any 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.

An Interim electronic device policy advised CBSA officers to notify individuals that they are permitted to change their device passwords if they are permitted to depart the customs control area with their devices intact.[122] While this guidance has been removed from the final version of the CBSA's electronic device policy,[123] it remains important practical advice to change any passwords provided to the CBSA immediately upon completion of a search. There should not be any legal impediments to doing so, unless the CBSA indicates otherwise.

119 Bolduc testimony http://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-69/evidence#Int-9671565

120 CBSA, PRG-2015-31, FINAL, updated February 28, 2017, *supra* note 2.

121 *Privacy at the US Border, supra* note 2 at 25.

122 CBSA, PRG-2015-31, INTERIM, issued June 30, 2015, *supra* note 2, p 4.

123 CBSA, PRG-2015-31, FINAL, updated February 28, 2017, *supra* note 2, p 4.

PHOTO CREDIT: TYLER LASTOVICH

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 and Delay

The CBSA may treat a refusal to provide a password as suspicious, and inspect your electronic device more carefully or ask probing questions. Legally, a refusal of this sort should not count as an 'indicator' of suspicion as the mere exercise of your rights should not provide a rationale for the state to invade you privacy.[124] Nonetheless, refusal to facilitate access to your device might informally encourage the CBSA to treat you with greater suspicion and encourage it to rely on other indicators to justify more intrusive searches.[125]

As noted above, CBSA officers are instructed not to compel individuals to provide passwords

124 *R v Gibson*, 2017 BCPC 237, para 188; *R v Chehil*, 2013 SCC 49, para 44.

125 See for example *R v Sandhu*, 2016 BCPC 397, para 54.

for remote accounts or content.[126] However, CBSA officers might still ask individuals to voluntarily log on to such accounts in order to verify claims made at the border. For example, one CBSA officer asked an individual seeking re-entry into Canada after a trip to the United States to log into his E-Bay account in order to demonstrate that the undeclared goods found in his car were purchased on the site and not during his trip abroad, as he had claimed.[127]

Even where refusing to provide access to a device might not contribute to suspicion, it may lead to additional delay. The CBSA may seek to deploy front-line forensic tools in order to access the device, might search your other luggage more carefully, or may subject you to additional questioning in order to fill in any gaps that might be left from your refusal to provide access to your device.

Denial Of Entry

If you are not a Canadian, there is a risk that you will be denied entry into the country if you do not cooperate with the CBSA. If you are a Canadian, CBSA is not permitted to deny you entry into the country even if you repeatedly refuse to comply with requests to unlock your devices or data.

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 be able to enter the country. 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 an officer cannot complete inspecting a device because a password is unavailable (or for unrelated technical difficulties), the device could be detained and sent to a specialist for a forensic examination or to specialized units who are adept at breaking passwords or bypassing encryption.[128] So a traveller risks losing access to their device, usually for a considerable time, if they withhold the password.

However, some court decisions suggest that the *Customs Act* does not permit the seizure of e-devices absent reasonable belief. For this

126 *R v Gibson*, 2017 BCPC 237; ETHI Testimony; CBSA, PRG-2015-31, FINAL, updated February 28, 2017, *supra* note 2.

127 *Ward v Canada (Minister of Public Safety and Emergency Preparedness),* 2014 FC 568.

128 CBSA 2015 ATI, *supra* note 2 at 6.

reason, a court found that "a search of a computer or other 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."[129] This might mean that the CBSA cannot seize your device solely on the basis that you have refused to provide a password to it, requiring an independent rationale for believing the device contains contraband or evidence of an offence.[130]

Nonetheless, there is no indication that CBSA policy has evolved to take this into account, so refusing to provide a device password might lead to its long-term seizure, regardless of the ultimate legality of such a seizure. In addition, you may not know if the CBSA has already formed the necessary suspicion to seize your device or not. For example, the CBSA officer might already have reason to think that an electronic receipt for an unreported imported good is contained on the mobile device.[131] So your persistent refusal to provide access to your phone might lead to its long term seizure regardless of the legal protections in place.

Arrest

As described above, refusing to facilitate access to your electronic device upon request means 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.[132] These penalties are theoretically available independently of whether any evidence of another crime is ever found on the device or not.

129 *R v Gibson*, 2017 BCPC 237, paras 47 and 188. For descriptions of the forensic and encryption bypass processes in question, see: *R v Ferguson*, 2018 BCSC 594 and Lex Gill, Tamir Israel & Christopher Parsons, "Shining a Light on the Encryption Debate: A Canadian Field Guide", May 2018, *CIPPIC / The Citizen Lab*, https://cippic.ca/uploads/20180514-shining_a_light.pdf, pp 81-84.

130 *R v Chehil*, 2013 SCC 49, para 44.

131 For example, see *Leslie v Canada (Public Safety and Emergency Preparedness)*, 2017 FC 119, paras 7 and 13 (border officer finds undeclared new clothing in car upon re-entry into Canada, searches phone suspecting proof that the clothing were purchased abroad and undeclared might be found on the device); *R v Cimini*, [2008] OJ No 5380 (ONCJ), paras 8-9.

132 *Customs Act,* supra note 3, s 153.1 and *Immigration and Refugee Protection Act, supra* note 13, 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.[133] There are a number of exceptions to this rule, however, including disclosure in accordance with another Act of Parliament.[134] 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,[135] including to prepare for criminal proceedings.[136] 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."[137]

CBSA may also disclose personal information collected during the examination of a traveller for the purposes of the *Security of Canada Information Sharing Act* ("SCISA").[138] The basic premise of the *SCISA* is to "encourage and

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

134 *Ibid,* s 8(2)(b).

135 *Customs Act, supra* note 3, s 107(4).

136 *Customs Act, supra* note 3, s 107(4)(a).

137 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>.

138 *Customs Act, supra* note 3, s 107(4)(i).

facilitate information sharing between Government of Canada institutions in order to protect Canada against activities that undermine the security of Canada."[139] 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."[140] 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."[141] 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."[142]

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. We know that Canada has intelligence sharing arrangements with foreign governments, but due to the lack of transparency in relation to such treaties,[143] 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 also be used as evidence in other 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.[144] If the request were made during the period in which the CBSA was allowed to keep the data, the CBSA might have been forced to turn over the data. If that had occurred, the contents of the defendant's laptop computer could have been used against him by someone other than the government in order to sue them in court.

According to CBSA policy, copies of data are not retained once the investigation is complete. The

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

140 *Ibid, s* 2.

141 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/>.

142 *Ibid,* at para 36.

143 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>.

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

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. When goods are 'forfeited' in this manner, the CBSA will typically seize the entire device as opposed to simply making copies of the contraband and will rarely return the device to its original owner. Once an investigation has been complete and the evidence is no longer needed, the CBSA destroys the digital devices by "drilling holes into electronic media or discs" and then making sure the data cannot be accessed.[145]

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.

145 CBSA ATI Volume 5, *supra* note 2 at p.4.

CHAPTER FOUR

Preclearance Areas

These are the areas in some Canadian airports, train terminals and ferry terminals where travellers departing for the Unites States clear their customs prior to leaving Canada. To implement an agreement with the United States, Canada has provided the legal authority through the *Preclearance Act* for United States Customs and Border Protection ("CBP") to operate in these areas as preclearance officers. Similarly, preclearance areas set up on US soil where the CBSA administers Canadian laws and customs processing 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 United States 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 those of the United States. 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*.[146] In other words, the officer does not need a warrant or even reasonable suspicion

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

to examine the information on your electronic device. While some United States appellate courts have held that suspicionless mobile device searches violate the Fourth Amendment which prohibits unreasonable searches and seizures,[147] it is not clear how these protections apply to Canadians seeking entry into the United States in general and through pre-clearance areas more specifically.[148]

The United States' CBP's 2018 Directive on the Border Search of Electronic Devices[149] 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 cat-

147 *US v Cotterman,* 709 F.3d 952 (9th Circuit, 2013).

148 Sophia Cope, Amul Kalia, Seth Schoen & Adam Schwartz, "Digital Privacy at the US Border: Protecting the Data on Your Devices", *Electronic Frontier Foundation,* December 2017, https://www.eff.org/files/2018/01/11/digital-privacy-border-12-2017.pdf .

149 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].

egorically 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 operating system or through other software, tools, or applications." [150]

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." [151] 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).

PASSWORDS

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 if a traveller chooses to answer a question, they must do so honestly.[152]

150 *Ibid* at para 5.1.2.

151 United States, Customs and Border Protection, "Border Search of Electronic Devices", CBP Directive No 3340-049A, January 4, 2018, https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf, section 5.1.4.

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

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.[153] 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 United States.[154]

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 United States 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.[155] If the officer believes on reasonable grounds that the device will provide evidence of an offence under Canadian law, the detention is mandatory.[156] 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.[157]

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.[158]

153 *Ibid, s* 16(3).

154 *Ibid, ss* 16(2) and 18.

155 *Ibid, s* 26(1)(a).

156 *Ibid, s* 26(2).

157 *CBP Search Directive, supra* note 149.

158 *Preclearance Act, supra* note 152, 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 is 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[159] 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.

159 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, is the stored data encrypted in a manner that prevents the service provider from accessing it? Do they require a warrant from law enforcement agencies before handing over copies of your information? Finally, if accessing the data from abroad while travelling, make sure data is transmitted in a secure manner, using end to end encryption or a Virtual Private Network.[160]

Turn Off Your Devices and Enter Airplane Mode

Before you go through customs, turn off your electronic devices and make sure none of your accounts or applications are set to automatically log in when activated. 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

160 For a description of key encryption concepts, see: Lex Gill, Tamir Israel & Christopher Parsons, "Shining a Light on the Encryption Debate: A Canadian Field Guide", May 2018, *CIPPIC / The Citizen Lab*, https://cippic.ca/uploads/20180514-shining_a_light.pdf.

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 (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 re moved from its casing, the security officers may prevent you from taking it on the plane.[161]

Before powering down your device, you should also enter it into 'airplane mode'. CBSA policy indicates that the border officials should place your phone in airplane mode prior to inspecting it because they are not permitted to search remote content and to prevent 'remote wipe' functionality from interfering with content already on the device. However, placing your device in airplane mode will ensure no data is inadvertently downloaded to the device upon activation during a border search. Taking the additional step of logging out of any social media, email, content streaming or remote storage accounts prior to crossing a border would further decrease this risk.

161 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>.

Require a Login Password and Encrypt Your Device

Your first line of defence in protecting against a search of your electronic device is to encrypt it and 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.

Bring Less Data

The best option for crossing the border is to bring no data at all. The easiest way to do this is, if possible, to travel without an electronic device at all or to use a dedicated travel device with no data or activity on it.

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 United States, your data can be accessed under the USA PATRIOT Act and the Foreign Intelligence Surveillance 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 compelled.

If you wish to avoid trusting 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.[162]

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 United States. This would include physicians, who cannot store any

162 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>.

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.[163] Before long, lawyers in British Columbia will have to be sure that their cloud service provider offer 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.

Secure 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 may become subject to a border search. This remains true for electronic devices, encrypted applications that store data on those devices, and for any individually encrypted files.

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 security of a password is a function of its length, randomness and complexity. The usual advice for creating passwords is therefore to use random character strings, of substantial length (at least 20 characters), and that are comprised of a mix of upper and lower case letters, numbers, punctuation and special characters (leading to high complexity).

Mathematicians and computer security experts have been encouraging a move away from this sort of password because it is hard for people to remember the dozens of random passwords they wind up collecting for all their online accounts without some form of password management software. As a result, people select random character strings that are too short and reuse the few passwords they remember for multiple accounts, increasing the risk that the password will become compromised.

163 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 dictionary words in an unusual sequence instead of a single word. This is allows individuals to use and remember many more passwords, each of much greater length than can be accomplished.

If you want or need a higher level of security, experts recommend the use of a password manager such as Keepass. These tools let you easily generate secure and fully random character strings and store these in a manner that is easily accessible whenever you want to access a specific account associated with a given stored password. In this way, you don't need to remember any specific passphrase other than that controlling access to the password manager itself.

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.

If compelled to choose a short password, 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. The use of random dictionary words is only secure if employed in a passphrase of sufficient length.
- That replace letters in dictionary words with commonly used replacement characters such as when '!' is used in lieu of the letter 'I' or '$' is used in place of the letter 'S'. Many password cracking mechanisms will include these commonly used variations when seeking 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. Similarly, if you are compelled to provide your password or phrase to the CBSA, you might compromise other services or applications employing the same password or phrase.

If you need help coming up with a strong password, many websites offer a password generating tools that mix and match random letters, numbers, and symbols to give a password that meets your needs. Software such as KeePass can be used to generate random passwords of any length and in a manner that complies with any service-specific character restrictions (for example, some services will not allow the use of punctuation or special characters). There are also online tools for generating random passphrases, such as the Electronic Frontier Foundation's random word list.[164]

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 (or a fragment of it) to your destination with somebody else, store it online, or give it to your lawyer or the security department in your company.[165] Similarly, if you are using a password manager, you can have a friend or colleague bring the encrypted password database file to your destination, have them transmit it to you once you've arrived or you can leave it with your lawyer until you return.

Not 'having' a password might lead to complications comparable to those experienced when you refuse to provide border officials with your password on demand. If you are travelling for work, an explicit corporate travel policy limiting carriage of passwords while travelling might help explain to border services why you do not have access to your passwords. If your password is entrusted with your lawyer or your company's technical security personal, you will still be able to choose to disclose this password to border officers, if required, by contacting the individual trusted with the password.

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 control of a physical device that

164 See: https://ssd.eff.org/en/module/animated-overview-how-make-super-secure-password-using-dice and https://www.eff.org/deeplinks/2016/07/new-wordlists-random-passphrases .

165 https://www.eff.org/wp/digital-privacy-us-border-2017

generates a random, one-time-use code each time you need to log in to that account.

If, as many do, you use your mobile device as the second factor (you can get the one-time code via text message or from an app installed on the phone), the two-factor principle may not actually provide a heightened barrier to access in the context of border searches. Use of a dedicated two-factor authentication mechanism (such as a 'Yubikey') might be more effective, however if this dedicated mechanism travels with you, you might still be compelled by border officials to provide access to a device or application.

However, in the case that your laptop or mobile device 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 to protect 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 securely stored on a device 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. Moreover, even if you are using strong encryption and a secure password or passphrase, there are many software and device security flaws that CBSA experts might exploit to bypass the encryption on your device altogether.

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's Enterprise or Pro editions 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.

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. Most modern iOS devices are encrypted by default. However, the default settings for some versions of iOS only rely on relatively weak 4 digit passcode that should be replaced with a more complex passphrase.[166] 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.

Even with strong encryption and a secure passphrase, no device is 100% secure. Various state agencies and third party vendors are constantly finding new ways to bypass encryption on the most popular and widely used mobile devices including iOS and Android, even as their manufacturers (Apple and Google, respectively) continually seek to secure any security gaps.

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. Similarly, some individuals might be particularly concerned about exposing their list of contacts. Journalists wishing to keep sources hidden and lawyers wishing to avoid disclosure of client lists might consider checking to see if

166 https://ssd.eff.org/en/module/how-encrypt-your-iphone

their phone is configured to store a copy of their contact lists on their SIM cards. Most devices will allow the user to indicate whether contact lists should be stored on the SIM card, or on the device where it is protected by the operating system's general encryption mechanisms.

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.

It may be wise to encrypt certain documents or files even if you are using full disk encryption. For example, if journalist source documents or sensitive commercial materials are independently encrypted, border services might have a more difficult time justifying compelled access to these sub-sets of encrypted documents. However, this is no guarantee.

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.[167] 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. Another option is to enclose all privileged materials in an independently encrypted container.

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.

Even if segregated, privileged materials might be compromised at the border. If the CBSA compels decryption of a laptop and copies all data on the device, data from a segregated privileged account might be copied alongside

167 CBSA ATI Vol 9, *supra* note 2 at 39 s 23.6.7.

all other data. If the CBSA believes that an encrypted container might contain contraband despite the assurance of its owner, it might compel decryption of that container.

Solicitor-Client Privilege in the CBSA Context

There is a strong argument that any material over which the client or the solicitor 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.[168] Where there is a suggestion of any degree 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."[169] 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.[170] 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

168 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>.

169 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>.

170 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>.

and notaries, so it is doubtful that legal clients, 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."[171] 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.[172]

Solicitor-Client Privilege and Other Sensitive Information in the Preclearance Context

A claim of solicitor-client privilege over materials on an electronic device will likely not shield them from examination by the 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 so that any privileged material is "handled appropriately while also ensuring that CBP accomplishes its critical border security mission." [173] 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."[174]

Other types of information recognized as 'potentially sensitive' include medical records, commercial information potentially subject to trade secrets, and journalist's work-related information.[175] Similar to privileged information, such 'sensitive' information will not insulate a given device from being searched. However, if identified, CBP officers are directed to consult

171 *R v Gibson*, *supra* note 12 at para 19.

172 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>.

173 CBP Search Directive, supra note 151 at para 5.2.1.2.

174 *Ibid* at para 5.2.1.3.

175 *Ibid* at para 5.2.2 – 5.2.3.

with CBP lawyers to see if any US federal law or CBP policy requires additional safeguards for this information. Canadian journalists have been refused entry into the United States for refusing to provide US border control officers access to their electronic devices on the basis that doing so might reveal confidential sources.[176]

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.[177]

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.[178] You are also required by law to unpack and present any goods you have with you to the officer for inspection.[179] While it is still unclear if this extends to your digital 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

176 https://www.nytimes.com/2016/12/02/business/media/canadian-journalists-detention-at-us-border-raises-press-freedom-alarms.html

177 *Customs Act, supra* note 3, ss 153, 160.

178 *Customs Act, supra* note 3, ss 153.1, 160.1.

179 *Customs Act, supra* note 3, s 13.

Customs Act requires passengers to cooperate with officers inspecting their goods when the officer "so requests". 180 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.181

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.

180 *Customs Act, supra* note 3, s 13.

181 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).

- You may be arrested. In 2015 someone was arrested and charged with the criminal offence of "hindering" for refusing to provide his password.[182]
- You may be able to cross the border without any further interference.

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 citizen of the United States, the preclearance officer can refuse to let you into the country.
- You may be flagged for heightened screening whenever you cross the United States border in the future.
- You may be able to depart for the United States 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.[183]

182 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>.

183 *Preclearance Act, supra* note 152, s 10(1).

CHAPTER SIX

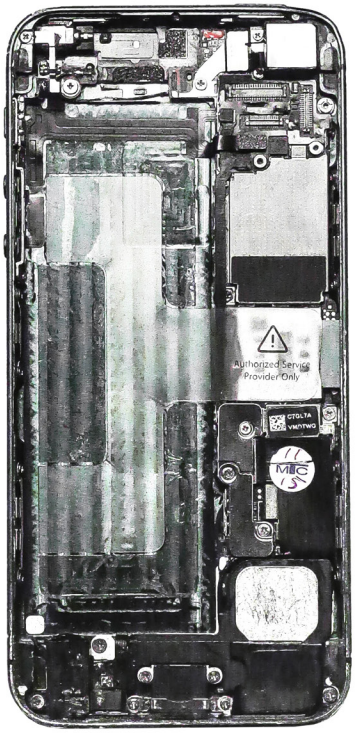
I've Been Searched!

Cleaning Up

If the CBSA or United States 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 United States 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.

However, you should note that there are many sophisticated tools that the CBSA might theoretically employ and that would not be removed by this process. If your work is sensitive and ongoing security is a serious concern, you should take your device to a security expert or simply get a new device.

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."[184]

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/

184 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 United States 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 nor 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 U.S. 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 bias 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 U.S. CBP practices and policies, developments in the law around border searches, and best practices for keeping your data secure.

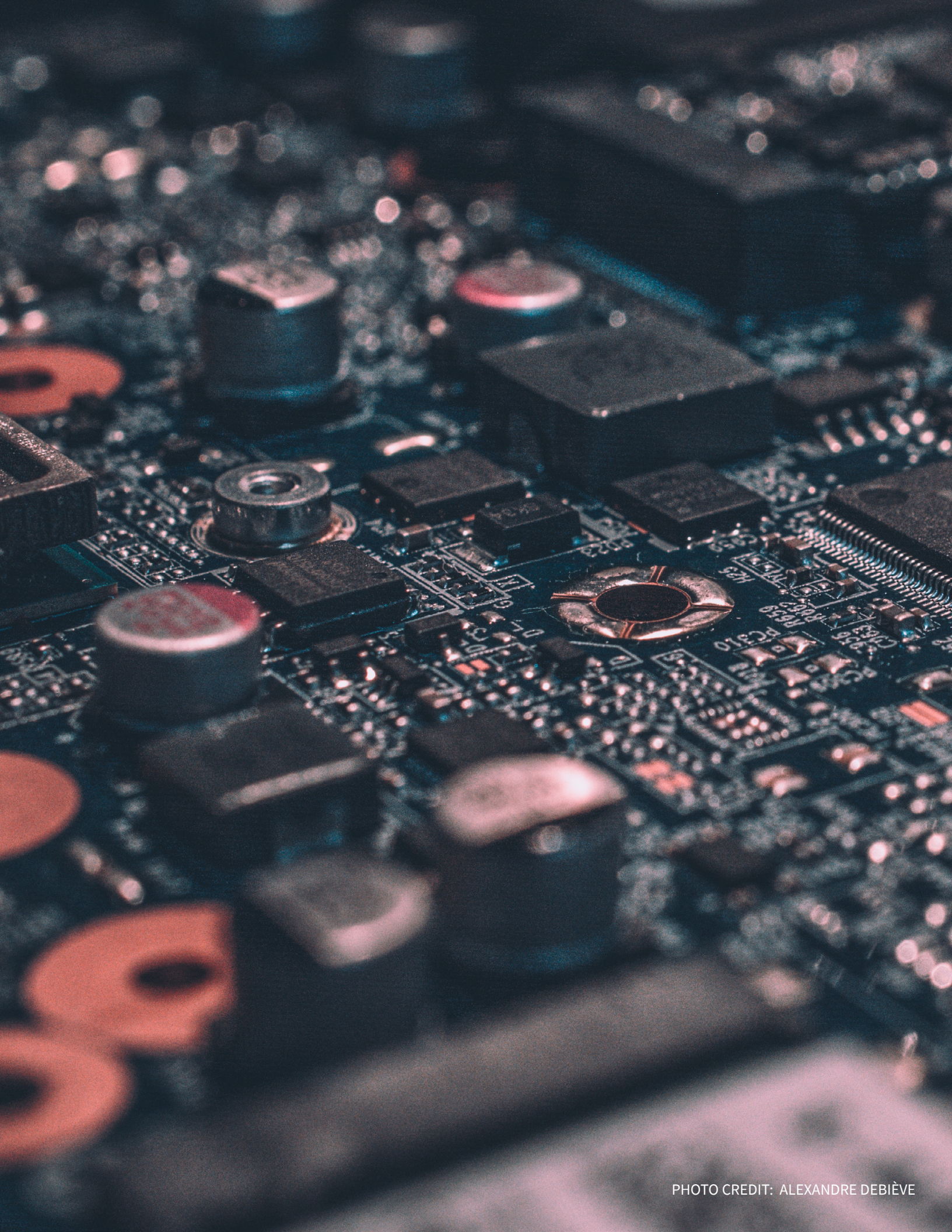


PHOTO CREDIT: ALEXANDRE DEBIÈVE

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

This project is funded by the Canadian Internet Registration Authority's (CIRA) Community Investment Program.

CIRA is building a better online Canada through the Community Investment Program by funding charities, not-for-profits and members of the academic community who are making the Internet better for all Canadians. CIRA is best known for our role managing the .CA domain on behalf of all Canadians. While this remains our primary mandate, as a member-based not-for-profit ourselves, we have a much broader goal to strengthen Canada's Internet. The Community Investment Program is one of our most valuable contributions toward this goal and funds projects in digital literacy, online services, research and infrastructure. Every .CA domain name registered or renewed contributes to this program. To date CIRA has contributed $5.45 million in Community Investment Program grants.

www.cira.ca

@ciranews

@cira.ca