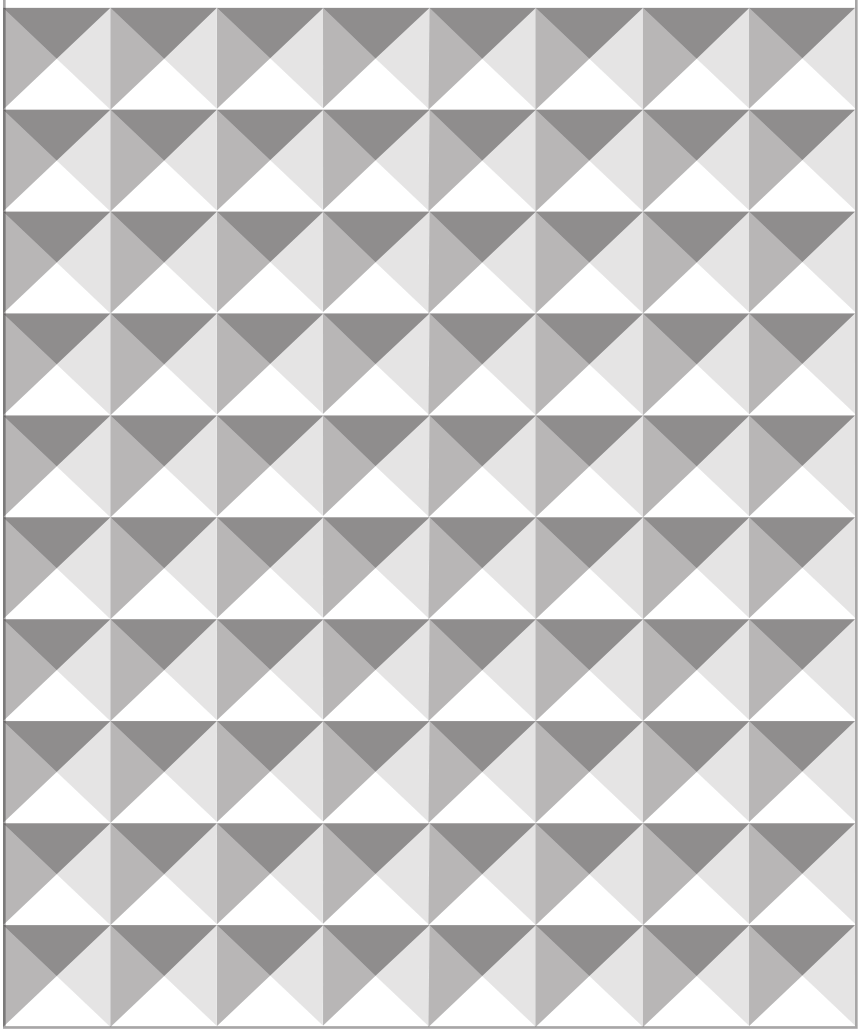
ELECTRONIC DEVICES

PRIVACY HANDBOOK

A GUIDE TO YOUR RIGHTS



BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION
BCCLA.ORG

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

Thanks to the Law Foundation of British Columbia for its support of this project.

The Law Foundation of British Columbia
1340-605 Robson Street
Vancouver, B.C. V6B 5J3
www.lawfoundationbc.org

B.C. Civil Liberties Association
550-1188 West Georgia Street
Vancouver, B.C. V6E 4A2
www.bccla.org

Written by Greg McMullen.
Design by Natalie Hawryshkewich 2011.

Cataloguing data available from Library and Archives Canada.

TABLE OF CONTENTS

1. INTRODUCTION

If you are like many Canadians, more and more of your daily life involves interacting with a digital 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 Kindle, and send emails from whatever device you happen to have with you at the time.

When you slip your phone into your pocket or laptop into your bag, it is easy to forget the volume of information you have with you all the time. It could easily be the digital equivalent of an entire filing cabinet. For many Canadians, it is an entire library – years of correspondence, business records, personal conversations, photos, web surfing history, 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.

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 instant messages, 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 – exactly the kind of data we keep on our digital 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 for a time when people could only bring a small amount of personal information with them, but seem out of date in a time when someone can bring every bit of personal data about them along in their pocket. This handbook is meant to help you make sense of this strange situation, and to protect your privacy when travelling with electronic devices.

WHAT THIS GUIDE DOES

This guide will explore three areas:

1. Rights at the border – What can and can't be done by a CBSA officer when he or she decides to search your electronic devices?
2. CBSA policies – What exactly do CBSA officers do when they are searching your electronic devices?
3. Best practices – What steps can you take to keep your data private and secure?
4. I've been searched! – What should you do if your electronic devices have been searched by the CBSA?

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

WHAT THIS GUIDE DOES NOT DO

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

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

Finally, this information only applies to crossing the border into Canada. Other countries have different policies. For crossing into the United States, see the Electronic Frontier Foundation's online guide to crossing the U.S. border: https://www.eff.org/document/defending-privacy-us-border-guide-travelers-carrying-digital-devices

2. RIGHTS AT THE BORDER

OVERVIEW

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

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

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.

THE *CUSTOMS ACT*

The *Customs Act* gives the CBSA broad powers to search both people and goods coming into the country.[1] This includes the things that people bring with them, even the files on your digital devices.

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

The *Customs Act* makes it clear that border guards have the ability to search "any document in any form" – including electronic documents.[2] Canadian

1 *Customs Act*, RSC 1985, c 1, s 99(1).

2 *Customs Act,* RSC 1985, c 1, s 2(1).

courts have found that files stored on electronic devices count as goods under the *Customs Act*, and that the CBSA has the power to search these documents.[3]

CBSA documents show that it treats computer files the same way it would treat a box of documents, claiming that "the only difference between a paper document and information stored electronically is the medium it is stored on."[4,5]

So far, Canadian courts have agreed with the CBSA. Despite the clear differences between the few paper documents in a travelers' 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.[6]

There have been hopeful signs that this view may be changing. In a recent decision from the Supreme Court of Canada, Justice Fish wrote that "[I]t is hard to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer."[7] It is not clear how this decision will affect future searches of electronic devices in the context of a border crossing, but it is a step toward greater protection of electronic devices in general.

---

3 *R v Leask*, 2008 ONCJ 25; *R v McDermin*, 2008 CanLII 68135 (Ont SCJ); *R v Whittaker* (2010), 946 APR 334 (NBPC).

4 In 2009, the BCCLA made a request for documents from the CBSA under the Access to Information Act. The BCCLA asked for policies on the search and inspection of electronic devices, statistics on the number and kind of devices searched, criteria used to select people for device inspection, policies for requesting and requiring passwords from individuals, and other information. The CBSA replied in early 2010, providing the BCCLA with several volumes of documents. While not all of our questions were answered, the documents helped develop our picture of how the CBSA conducts searches of electronic devices. Full details of the request and the response provided by the CBSA is available on the BCCLA National Security Blog, along with copies of the documents provided. http://nationalsecurity.bccla.org/2010/05/03/cbsa-laptop-search-documents/

5 CBSA ATI Volume 2, p 5. See footnote 4 for details.

6 *R v Leask*, 2008 ONCJ 25 at para 100.

7 *R v Morelli*, 2010 SCC 8 at para 3.

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 not the case during a border crossing.

At the border, the CBSA can search anything carried by a person. In the past, this has included brief patdowns of a travelers' clothing,[8] detailed searches of luggage,[9] or reading a traveler's bankbook.[10] 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 Section 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. While the CBSA should not single you out for search based on markers such as race, gender or religion, they may do so anyway, and courts have yet to put a limit on such profiling.

To date, no court cases have put limits on the searches of digital devices that can be conducted by the CBSA. However, the CBSA documents obtained by the BCCLA indicate that the CBSA hopes to avoid challenges to their search powers, so may be limiting searches to what they believe is allowed by the Charter.[11]

8 *R v Simmons* [1988] 2 SCR 495 at para 84.
9 *R v Hardy* (1995), 103 CCC (3d) 289 (BCCA).
10 *R v Jones*, 1992 CanLII 1096 (BCSC).
11 CBSA ATI Volume 9, p 36-37.

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.[12] 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.[13] 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.

SUMMARY

When you are crossing the border, if the CBSA decides to search your electronic devices, there is nothing you can do about it. The real work to be done 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 section will tell you what you can expect from a search by the CBSA. The last section will tell you what steps you can take to keep your data out of the hands of the CBSA if you do get searched.

12 CBSA ATI Volume 4, p 10 at s 42.

13 *R v Sekhon*, 2009 BCCA 187 at para 91.

3. CBSA POLICIES

While detailed information about CBSA policies for searches of digital devices is still limited, an Access to Information request made by the BCCLA in October 2009 shed some light on the subject. These documents provided information on how the CBSA chooses people to search, how those searches are done, and what happens to the data they collect.[14]

The next section will provide information about each of these areas, so when you get to the border you will know what to expect.

LEVEL ONE: INITIAL SEARCHES

The CBSA can and does search electronic devices, including laptop computers, cellphones, cameras, smartphones, and storage mediums like CDs, DVDs, and Flash drives.

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 digital 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.[15]

Generally, CBSA officers are looking for obscenity – hate literature or illegal pornography. 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.[16]

In recent years there have been rumors that the CBSA will be given increased powers to search for bootlegged copies of movies, including on travellers' personal electronic devices. These powers have not yet been put in place. It is

14 To read those documents, go to: http://nationalsecurity.bccla.org/2010/05/03/cbsa-laptop-search-documents/

15 CBSA ATI Volume 9, p 2 at slide 5.

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

not clear how CBSA officers could determine whether a particular MP3 was legally purchased or an infringing copy.

Sometimes, CBSA officers will look for other documents as well, including documents that show political opinion. For example, Amy Goodman, an American journalist, saw her laptop computer searched for anti-Olympic materials when coming to give a speech in Vancouver before the 2010 Winter Olympics.

If the CBSA officer sees something he or she feels needs a closer inspection, a slightly more thorough search can be conducted. This is not a forensic evidence-gathering mission. It is a slower look through the contents of a digital device.

TOOLS OF THE TRADE

The CBSA sometimes uses special software or hardware to help with a search of an electronic device.

For computers running Windows, the CBSA may use a program called "IC-What-UC" to scan for image files. This program runs from a CD and finds all of the image files stored on a computer, including images stored in a web browser's cache. The BCCLA's tests of this software show that it works as indicated, although it has some major weaknesses. If the browser cache is emptied or images are deleted and emptied from the "Recycle Bin", they will not be detected by IC-What-UC.

For Flash drives, CDs, and DVDs, the CBSA has special media viewer hardware that they use to quickly scan through the contents of these devices. The media viewer is essentially a DVD drive and card reader hooked up to a small screen.[17] This device allows CBSA officers to quickly view the contents of many common forms of media.

These are front-line tools designed to make the job of inspecting computers easier for officers who are not trained in computer forensics. More sophisticated tools are available to the highly trained officers who conduct detailed searches.

17 CBSA ATI Volume 4, p 24-26.

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 will be asked for your username and password, but again, CBSA policy states that you are not required to give it, unless a Court orders you to.[18]

CBSA specialists use a variety of techniques to search digital devices, including copying of data from your digital 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.[19]

Evidence collected by the CBSA can also be used as evidence in other cases. Recently, 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.[20] If the request were made during the period in which the CBSA was allowed to have the data, the CBSA would have been forced to turn over the data. The contents of the defendant's laptop computer could have been used against him by someone other than the government.

18 CBSA ATI Volume 7, p 8.
19 CBSA ATI Volume 9, p 36-37.
20 *Obégi Chemicals LLC v Kilani*, 2011 ONSC 4636 at para 33.

Taking disc images also allows the CBSA to run password-cracking software to try and access any data you did not provide a password to access.[21] Over a long enough timeframe any password can be broken, but using a strong password makes the process much more time consuming, to the point that it is all but impossible. An extremely strong password can take hundreds of years to break, even on the best supercomputers.

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

Not every border crossing has computer search specialist on staff. Often, electronic devices will have to be detained to give the officer time to conduct a full search of the device. However, CBSA officers have been trained to return electronic devices as quickly as possible to avoid challenges to current CBSA practices.[22] 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.

According to CBSA policy, copies of data are not retained once the investigation is complete. The CBSA, however, has refused to release information on how data is destroyed after collection, except when goods are made "forfeit" because they contain contraband like child pornography or hate literature. Goods that are forfeit are seized by the CBSA and never returned to their original owners, and would likely be the original devices, not the copies. Once an investigation has been 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.[23]

RANDOM SEARCHES

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

21 CBSA ATI Volume 7, p 8.
22 CBSA ATI Volume 9, p 36-37.
23 CBSA ATI Volume 5, p 4.

The CBSA has refused to release information about the number of people who are searched every year at Canadian border crossings. It is not clear how common searches of electronic devices are, but as more people bring these devices with them across the border, it is safe to assume that the number of searches is increasing.

TARGETED SEARCHES

Most of the people searched by the CBSA are not chosen at random, but rather by various criteria 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.

The CBSA has not publicly disclosed a complete list of the indicators it uses to select people for targeted searches. However, the documents released in response to the BCCLA's Access to Information request give some hints, and news reports of people caught crossing the border with child pornography or other banned materials fill in some of the blanks.

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

- Are importing something the CBSA deems to be suspicious.[24] 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".[25]
- Have travelled to and from "high risk" destinations.[26] 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, and Spain.
- Are a single man traveling alone.[27]

24 CBSA ATI Volume 4, p 6, at s 32.
25 CBSA ATI Volume 6, p 13.
26 CBSA ATI Volume 4, p 6, at s 32.
27 Alison Auld, "Pope appoints new bishop for troubled N.S. diocese", *The Hamilton Spectator*, November 19, 2009. http://www.thespec.com/article/677123

- Demonstrate "an interest in Pornography".[28] 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.[29]

PASSWORDS

If your electronic devices are searched, the CBSA will ask you to provide any passwords required to access the information on digital devices.[30]

According to the documents obtained by the BCCLA, the CBSA will ask for a password if one is required, but will not insist that it be provided. We believe that refusing to provide a password is within your rights under Canadian law.

However, this has not been tested in Canadian courts, and it is not certain that the courts will agree.

The CBSA may treat a refusal to provide a password as suspicious, and inspect your electronic devices more carefully or ask probing questions. 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. Take this into consideration when deciding whether or not to offer up your password.

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.

If you do not provide your password, you increase the chances that your electronic devices may be detained or seized for further inspection. Your data may be copied and retained by the CBSA. Of course, providing a password does not guarantee that your electronic devices will not be detained or seized.

28 CBSA ATI Volume 9, p 3 at slide 9.
29 CBSA ATI Volume 4, p 6, at s 32.
30 CBSA ATI Volume 7, page 8.

This section is limited to the law in Canada as it stands today. Other countries may require that you provide a password to a border guard upon request. For instance, in the United Kingdom, a man was recently jailed for refusing to provide his password to police.[31] In the U.S., border guards cannot force you to turn over your password, but unless the Fifth Amendment applies, a judge can.[32]

31 Daily Mail Reporter, "Teenager jailed for refusing to give police his computer password", *The Daily Mail*, October 6, 2010. http://www.dailymail.co.uk/news/article-1318103/Teenager-jailed-refusing-police-password.html

32 "EFF's Guide to Protecting Electronic Devices and Data at the US Border", Electronic Frontiers Foundation, November 24, 2010: https://www.eff.org/deeplinks/2010/11/effs-guide-protecting-devices-data-border

4. 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.

While the tips here have what we know about CBSA searches in mind, the technological know-how will help you prepare for crossing the border into other countries, and help you become more security-conscious in general.

MAKE A BACKUP

One of the most important things you can do before traveling is to make a full backup of your digital devices. This backup should not cross the border with you. Making regular backups is a good habit to be in anyhow, in case your digital 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 digital device is detained for an extended period.

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

TURN OFF YOUR DEVICES

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

Getting into the habit of turning off your digital devices before going across the border will also make sure that you are logged out, and that when the CBSA 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.

REQUIRE A LOGIN PASSWORD

Your first line of defence in protecting against a search of your electronic device is to require a password to log on. This simple step will keep a CBSA 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 CBSA officer your password if asked, it is a good practice to keep your electronic devices password protected. An 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.

Note that a simple screen lock password is not a proper replacement for full disc 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 disc encryption or file encryption, below.

BRING NO DATA

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 CBSA to search. However, this option comes with the obvious disadvantage of being left without your electronic device once you reach your destination.

If you securely erase all the data from your electronic device, you will keep your data private. However, you may still be subjected to a search of your devices.

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 device just 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 digital 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 disc encryption, which is discussed later.

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 without a warrant. Providers like Dropbox keep the encryption key to your data. They can and will turn your data over to law enforcement if it is requested.

Some cloud providers offer more security, storing data so even their own employees cannot access it without your password or passphrase:

- **Spideroak** https://spideroak.com/ and **Wuala** www.wuala.com/ are essentially the same as Dropbox, allowing you to drag and drop files to the cloud from your electronic device. The big difference is that Spideroak and Wuala encrypt your data before sending it, so your data stays secure.

- **BoxCryptor** http://www.boxcryptor.com/ encrypts any folder on your computer as you use it. If you choose your Dropbox folder, those files will be encrypted before being uploaded to Dropbox.

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 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.[33] Before long, lawyers in B.C. 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.

STRONG PASSWORDS

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

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

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

33 "Report of the Cloud Computing Working Group", Law Society of British Columbia, January 27, 2012: http://www.lawsociety.bc.ca/docs/publications/reports/CloudComputing_2012.pdf

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

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

Don't use passwords:

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

If you need help coming up with a strong password, many websites offer a password generating tools that mix and match random letters, numbers, and symbols to give a password that meets your needs. Some examples include:

Gibson Research Corporation's Password Generator: https://www.grc.com/passwords.htm

Diceware: https://secure.wikimedia.org/wikipedia/en/wiki/Diceware

FULL DISC ENCRYPTION

If you need to bring your data with you, the safest way to do so is with full disc encryption. Full disc encryption essentially scrambles the contents of your electronic device. The data is unlocked by a passphrase.

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

Security experts recommend that you choose a password made up of a series of randomly selected words or a strange phrase. We strongly recommend using a program like Diceware to randomly generate a passphrase to use for your encrypted disc. If you use a weak password for your encrypted disc, you are taking a risk that it will be cracked.[34]

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

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

The Ultimate Editions of Windows Vista and Windows 7 come with BitLocker, full disc encryption software that can be activated in the Control Panel.

Apple computers running OS X 10.7 or later have full disc encryption built in. You can enable full disc 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

34 Cory Doctorow, http://boingboing.net/2011/08/10/xkcd-on-the-password-paradox-human-factors-versus-computers-brute-force.html

for your documents and files stored in that folder, but your applications, system files, and other users' documents will still be accessible.

If your computer does not have disc encryption software pre-installed, you can try TrueCrypt, a free, open source disc encryption tool. TrueCrypt supports many advanced security features, such as hidden operating systems and partitions. TrueCrypt is for more advanced users, so before you use it to encrypt your data, be sure you have read the instructions carefully.

Unfortunately, most handheld devices do not offer strong protection. Apple's iOS 4 devices feature strong encryption, but Elcomsoft, a Russian security company, has demonstrated how to break that encryption.[35] Full device encryption is currently available on some Android phones, but not all of them. Blackberry phones are still the most secure, but Elcomsoft has also shown that Blackberry backups can be broken even more easily than iPhone encryption.[36]

FILE ENCRYPTION

If full disc 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, or 7, 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.

35 MSNBC Technolog, "Russian forensics firm cracks iPhone encryption", May 24, 2011. http://technolog.msnbc.msn.com/_news/2011/05/24/6709033-russian-forensics-firm-cracks-iphone-encryption

36 John E Dunn, "Blackberry backup encryption broken by Russians", NetworkWorld, October 4, 2010. http://www.networkworld.com/news/2010/100410-blackberry-backup-encryption-broken-by.html

Mac OS X allows you to create an encrypted disc image. Open the Disk Utility application, then press the New button. Enter a name for the disc image, and select a place to save it. Choose a disc 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 disc image to open it, then enter your password. It will appear like a disc on your desktop, and any files you put inside it will be encrypted.

Again, if you do not have access to these tools, or prefer something with more options, a program like TrueCrypt is an excellent choice. However, this type of program is for more advanced users, so user beware.

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 the CBSA at all, except to verify that it is what it claims to be. 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.[37] However, this is made much more difficult if privileged materials are mixed in with unprivileged materials.

37 CBSA ATI Volume 9, p 39 at 23.6.7.

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

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

CLEANING UP

If the CBSA 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. Even if you have taken the precautions above, your computer may now be host to what the Canadian Bar Association has called "Fedware" – software designed to snoop on your computer usage and report back to the CBSA or other law enforcement agencies.[38]

CBSA 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.

The BCCLA has not seen any evidence to suggest that the CBSA is actually installing monitoring software on the computers it searches, but with data security it is better to be safe than sorry. Law enforcement agencies in other countries have come under fire for installing Fedware. For example, German police were found to be installing Fedware that could give police complete control of suspects' computers.[39]

If you suspect that you may be infected with Fedware, 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

38 Luigi Benetton, "How to Secure Your Laptop Before Crossing the Border", CBA Practice Link, August 2009: http://www.cba.org/cba/practicelink/tayp/laptopborder.aspx

39 BBC News, "Germany Spyware: Minister calls for probe of state use", October 11, 2011: http://www.bbc.co.uk/news/world-europe-15253259

increasingly being used to store software that sticks around even after you wipe your system clean.[40]

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 Fedware, running an antivirus is still an important step to take in reassuring yourself that your digital device is not passing your data along to third parties.

CALLING IT IN

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

Unfortunately, the only place to file an official complaint about a CBSA search is to the CBSA itself. While it is unlikely that your report will have any impact on CBSA policy on its own, if enough people complain, policy might change. You can make your complaint here: http://www.cbsa.gc.ca/contact/feedback-retroaction-eng.html

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.

If you have been searched by the CBSA, report it to the BCCLA at info@bccla.org or by calling 604-687-2919. The more we know about CBSA policy, the better we can make this handbook as we update future versions online.

40 Hon Lau, "Are MBR Infections Back in Fashion?", Symantec Official Blog, August 8, 2011: http://www.symantec.com/connect/blogs/are-mbr-infections-back-fashion-infographic

6. CONCLUSIONS

Eventually, the law around border searches will catch up with the way that Canadians are using their digital 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 practices and policies, developments in the law around border searches, and best practices for keeping your data secure.

Special thanks to the following individuals for sharing their expertise and reviewing early drafts:

Jesse Brown – TVO Search Engine
http://jessebrown.ca

Cory Doctorow – Boing Boing
http://boingboing.net

Vincent Gogolek – BC Freedom of Information and Privacy Association
http://fipa.bc.ca/

Colin Keigher – Vancouver Hack Space (VHS)
http://vancouver.hackspace.ca/wp/

Christopher Parsons
http://www.christopher-parsons.com

Catherine Middleton – Ryerson Broadband Research
http://broadbandresearch.ca/

Seth David Schoen and Lee Tien – Electronic Frontiers Foundation (EFF)
https://eff.org

The BCCLA gratefully acknowledges support from the Law Foundation of British Columbia for funding this handbook.

If you are like many Canadians, more and more of your daily life involves interacting with a digital device. Increasing amounts of personal information are being stored on portable electronic devices. This handbook discusses your rights to privacy in your electronic devices when crossing international borders into Canada, and sets out best practices on how to keep your data secure.

Written by Greg McMullen
Published by the B.C. Civil Liberties Association
Funding provided by the Law Foundation of British Columbia

THE LAW FOUNDATION OF BRITISH COLUMBIA

bccla
BC Civil Liberties Association