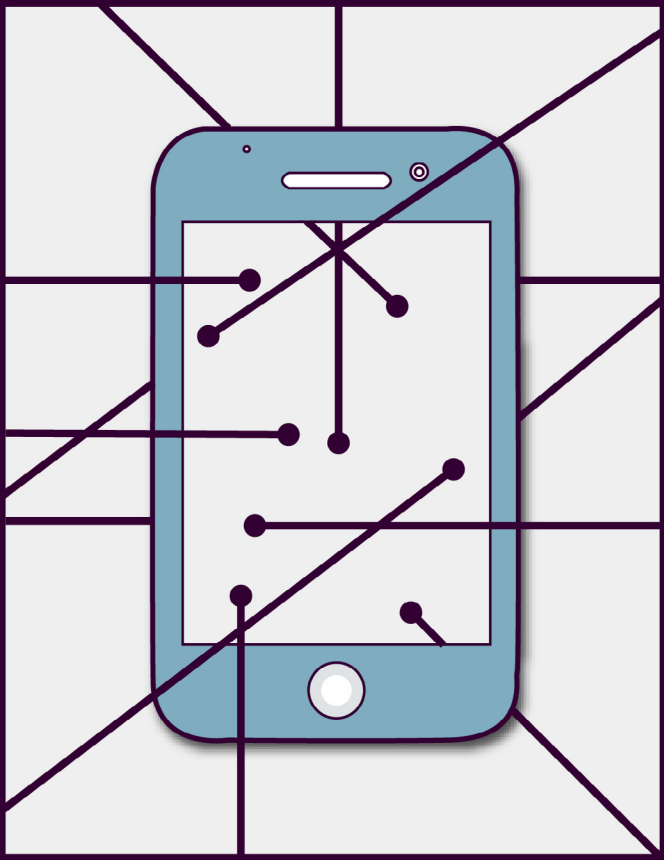
Electronic Devices Privacy Handbook

A SHORT GUIDE TO YOUR RIGHTS AT THE BORDER



BC CLA

cippic

This guide will inform you about your privacy rights related to your devices – such as laptops, cellphones, and tablets – at the border. It's aimed at people crossing the border into Canada or departing for the U.S. through preclearance areas in Canada.

Usually, the police cannot search randomly without suspicion, but this isn't the case at the border. The Charter of Rights and Freedoms applies at the border, but the 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 Customs Act gives the Canadian Border Services Agency (CBSA) broad powers to search people and goods coming into the country, including the things that people bring with them. This includes the content – the files, photos and videos – on your digital devices. The files on your devices are "goods" under the Customs Act, and border officers can search goods coming into Canada without a warrant – even if they have no reason to suspect that the goods are or contain contraband.

Non-citizens seeking to enter Canada, including asylum seekers, may be subject to searches as well. Under the Immigration and Refugee Protection Act, a CBSA officer may search the luggage and personal effects of a person seeking to come to Canada at a port of entry, including electronic devices and media. However, the officer must have:

- reasonable grounds to believe that the person has not revealed their identity or has hidden on their person documents that are relevant to their admissibility, or

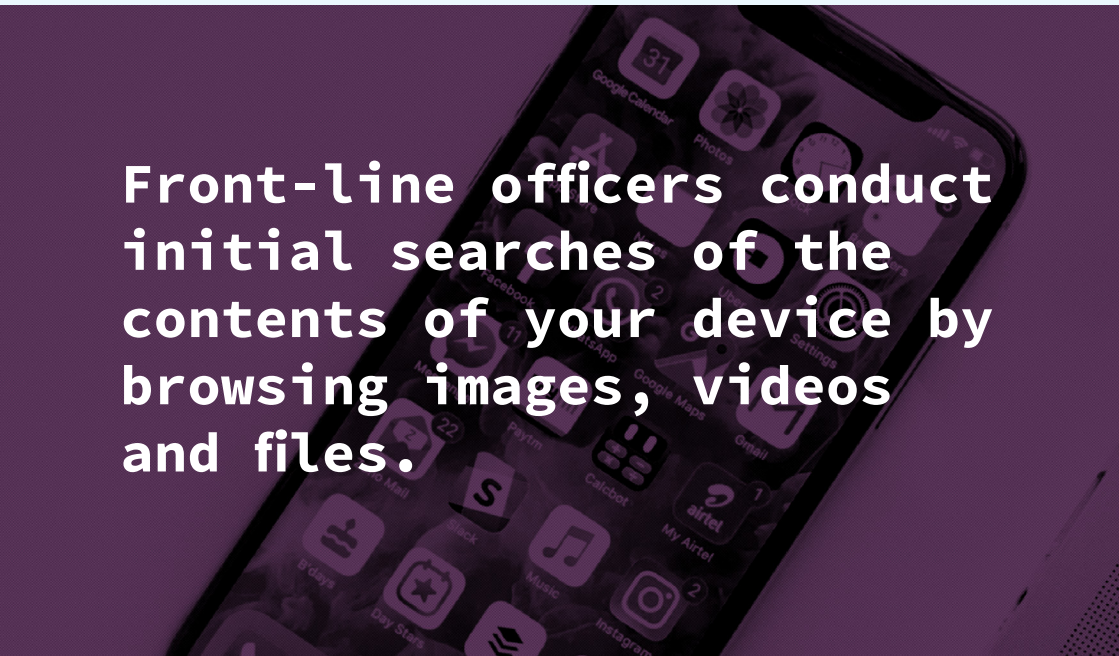
- reasonable grounds to believe that the person is involved with people smuggling, human trafficking, or document fraud.

Searches of devices must be limited to identifying the person, finding documents relevant to admissibility, or evidence of the offences outlined above.

Front-line officers conduct initial searches of the contents of your device by browsing images, videos and files. This is meant to be a cursory look at the contents to determine that they do not contain contraband – such as child pornography or hate literature – or evidence of a crime. Initial searches can be random or targeted.

Anyone can be subject to a random search. There is concern that travellers are targeted for searches based on their 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. If you believe you have been discriminated against, more information on filing a complaint can be found below.

Most of the people searched by the CBSA are not chosen at random, but rather through targeting. People are targeted based on information in travellers' databases – particularly for air, rail or cruise ship arrivals – as well as "indicators" that the Agency thinks increase the likelihood that a person's electronic devices will contain some form of contraband.



There is no publically available list of the indicators that the Agency uses, but anecdotally, you are more likely to be chosen for searches if you:

- Are importing something the CBSA deems to be suspicious, or are associated with known importers or exporters of materials the Agency objects to. This could include anime and manga, which the Agency is highly suspicious of
- Have travelled to "high risk" destinations (while no list is available, this likely includes destinations in Southeast Asia, as well as Germany, Cuba and Spain)
- Are a single man traveling alone
- Exhibit nervousness or agitation
- Have multiple electronic devices (including hard drives)
- Demonstrate an interest in pornography, as indicated by filenames or folders on your device
- Purchase a ticket to travel at the last minute
- Have coding on your suitcase that doesn't match where you are coming from
- Have unusual travel routes

During an initial search, officers should not carefully read every document or examine every photo on your device. They should only look at the contents for long enough to determine that they do not involve contraband (such as child pornography), or to confirm or settle suspicions about a violation of customs or immigration law. Information found during an initial search may be used to justify a more detailed examination.

Officers should only look at content that is already on your device. They are supposed to put the device in airplane mode and only look at local content (this includes emails and text messages that are marked "read"). The CBSA claims that it will obtain a warrant from a judge to search information that is only accessible remotely. However, the CBSA has been known to ask a traveller to voluntarily log into a remote account, so travellers cannot categorically expect linked social media accounts to remain private when crossing the border.

Detailed Searches

If an officer finds something they feel warrants closer inspection, a more thorough search can be conducted. These searches are carried out by specialists with expertise using forensic tools.

For a detailed search, your device will be taken out of your possession. The Customs Act gives the CBSA the power to detain goods if an officer is not satisfied that the goods have been properly screened for admission into Canada. Officers can also copy the entire contents of your device. This allows the CBSA to later run password-cracking software to access anything you did not provide a password for.

According to the CBSA, copies of the data are not retained after the investigation is complete. However, we know that the CBSA can and does share personal information that it collects from examinations with other government agencies such as the RCMP and with security agencies such as CSIS (who may in turn share it with foreign governments for intelligence purposes).

PHOTO CREDIT: TYLER LASTOVICH

PHOTO CREDIT: NEON BRAND

Passwords

Officers may ask you for your password or fingerprint to access the information that is stored on your device. There is uncertainty as to whether you are legally obligated to provide it, though the CBSA has been able to arrest people or threaten arrest for failing to provide the password. The CBSA maintains that they have the right to arrest people for failing to provide a password, and that they may do so where an officer has good reason to believe there could be prohibited material on a device.

The CBSA's position in 2017 was that it may not compel passwords to gain access to any account, file or information that is stored remotely. If you are asked for a password to access an online account, then, you should not face any repercussions for refusing to share it.

If you are asked and you choose not to disclose your password or provide your fingerprint to access information that is stored on your device, you risk increasing the CBSA's suspicion about the contents of your device, denial of entry if you are not a Canadian citizen or permanent resident, detention or seizure of the device for more detailed inspection by forensic specialists (which could take months), or arrest. Hindering or obstructing a CBSA officer is an offence that can carry fines of up to $50,000 and/or a term of imprisonment for five years.

U.S. Preclearance Areas in Canada

U.S. Customs and Border Patrol officers are authorized to administer U.S. law in parts of Canadian airports, train terminals and ferry terminals where travellers departing for the U.S. can clear U.S. customs prior to leaving Canada. In these areas, the administration of U.S. laws is subject to Canadian human rights laws, including the Charter of Rights and Freedoms. This means that Canadian search and seizure standards apply rather than U.S. ones. However, it is unclear if U.S. border officers have knowledge and training of the appropriate legal standards.

For searching electronic devices, U.S. laws are similar to Canadian laws: officers do not need a warrant or even reasonable suspicion to look at your phone. This should be local content only, and nothing that requires a network connection to see.

U.S. border officers perform basic and advanced searches. Basic searches can be performed with or without suspicion and involve any search of an electronic device that falls short of an advanced search.

PHOTO CREDIT: ALEJANDRO MOLINA FERNANDEZ

In an advanced search, the device will be connected to external equipment in order to gain access to the contents but also potentially copy them. Advanced searches require a reasonable suspicion of the violation of U.S. laws, or a national security concern.

U.S. border officers may ask you for your password. If you do not provide it, the officer may refuse to preclear you for departure to the U.S. The officer may also detain the device so they can perform a more advanced search. They should not keep your device for longer than five days, but reports show that sometimes devices are kept for many months.

Tips

In considering which actions you take to protect your privacy, be aware that your interaction with a border officer may escalate if they detect that you have deliberately tried to thwart a search, especially in a manner that destroys data that you otherwise would have been able to access, or if you have concealed the fact that the data is present at all.

- **Leave your devices at home** if you don't need them on your trip or use a dedicated travel device with no data or activity on it.

- **Make a backup of your data** before you cross the border and leave it home. This will be important if your device is detained or seized, but it also gives you the option of deleting unnecessary data from your device before you cross. You may also wish to clear the entire contents of your device before you cross the border and restore it from a backup afterwards.

- **Securely delete data** you do not need to travel with. This means not simply putting it in the recycling bin, but using built-in tools in Windows (a tool called cipher), Mac ('secure empty trash' or srm), or Linux (shred or srm) to permanently delete data. Be aware that border agencies have access to sophisticated forensic tools and may see information about deleted data that the average person can't. Just because you press "delete" does not guarantee that the information cannot be found by a border official.

- **Require a password** to log on or access your device. An officer who is only slightly curious and turns on your electronic device intending to browse the contents may lose interest when they realize they will have to ask you for your password.

- **Create a secure password**, for example by using several random words (a 'passphrase') if possible and avoiding passwords that are easy to guess.

- **Turn off your computer** before you go through customs, and make sure none of your accounts or applications are set to automatically log in when activated

- **Use two-factor authentication**, in the event that the border agency seizes one device but not the other.

- **Use Full-Disk Encryption** and require a strong passphrase to access it. Many new devices have this option built-in. This can keep your data safe from even the most experienced analysts. However, it is not clear what will happen if your electronic device is detained and the border agency is not able to access your data. Your device may be seized and not returned.

- If you do not opt to use Full-Disk Encryption, you can **encrypt specific critical documents** or files using built-in software as well.

- **Separate privileged and confidential documents** into their own folder to make it clear they are privileged. This includes lawyers' files, and can sometimes include files of doctors, psychologists and psychiatrists, and journalists. Border officers are supposed to take precautions not to look at privileged materials when warned that those materials exist, except to verify that it is what it claims to be. In theory, they should not look at privileged files at all, but border officers may not respect the law in this area.

PHOTO CREDIT: RAW PIXEL

PHOTO CREDIT: OWEN SPENCER

Filing a Complaint

If you think your search was improper, but your complaint is not about discrimination or an invasion of privacy, you can complain to the Canadian Border Services Agency itself. If your device has been seized, or you have been issued a penalty or fine, you can request a review of the decision.

You can also send written feedback to the Recourse Directorate of the CBSA, which can review officer conduct. Make sure to include all relevant information so a recourse officer understands your complaint and can get back to you.

If you believe you have discriminated against by a CBSA officer, you may be able to file a complaint with the Canadian Human Rights Commission. Grounds of discrimination include race, national or ethnic origin, colour, religion, age, sex, sexual orientation, gender identity or expression, marital status, family status, disability, genetic characteristics, or a conviction for which a pardon has been granted or a record suspended.

If you feel the CBSA has invaded your privacy, 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.

You may also wish to report any relevant incidents to interested civil rights groups in Canada including the International Civil Liberties Monitoring Group and/or the National Council of Canadian Muslims.

If you think that your privacy has been breached or if you have been discriminated against by U.S. officers in preclearance areas, we recommend writing to the Minister of Public Safety and the Minister of Foreign Affairs. You can also contact the Office for Civil Rights and Civil Liberties at the Department of Homeland Security, the Chief Privacy Officer of the Department of Homeland Security, and the Department of Homeland Security Traveler Redress Inquiry Program. You may also wish to report any relevant incidents to interested civil rights groups including the Electronic Frontier Foundation, the Council on American-Islamic Relations, and the American Civil Liberties Union.

BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

www.bccla.org @bccla @BCCivLib

cippic

www.cippic.ca @cippic

cira

BUILDING A BETTER ONLINE CANADA

This project was supported by a grant from the Canadian Internet Registration Authority's (CIRA) Community Investment Program.