DENTONS

The definitive guide for Canadians travelling to the United States

Introduction

On January 20, 2025, Donald Trump became the 47th President of the United States. On the same day, President Trump issued numerous Executive Orders related to the subject of immigration. For example, Executive Order 14161 (*Protecting the United States from Foreign Terrorists and Other National Security and Public Safety Threats)* requires the Secretary of State, in coordination with the Attorney General, the Secretary of Homeland Security and the Director of National Intelligence, to promptly:

- Re-establish a uniform baseline for screening and vetting standards and procedures, consistent with the uniform baseline that existed on January 19, 2021 (the last day of his first term), that will be used for any alien seeking a visa or immigration benefit of any kind;
- Vet and screen to the maximum degree possible all aliens who intend to be admitted, enter or are already inside the United States, particularly those aliens coming from regions or nations with identified security risks; and
- Evaluate all visa programs to ensure that they are not used by foreign nation-states or other hostile actors to harm the *security, economic, political, cultural or other national interests of the United States*.

These Executive Orders have already resulted in more aggressive inspections at the border. For example, Jasmine Mooney, a Canadian citizen, was recently sent to a detention center for nearly two weeks when she applied for a work permit at the US-Mexico border. Two German citizens were also recently sent to a detention center when they applied for admission to the United States because the border officers did not believe that they were legitimate visitors. In addition, Becky Burke, a citizen of the United Kingdom, was recently sent to a detention center in Washington State when she applied for re-admission to the US as a visitor, after being turned back at the Canadian border.

These highly publicized incidents have created a great deal of uncertainty for Canadians, who worry what might happen if they travel to the United States. So, what can be done to minimize potential issues when traveling to the United States?

Avoiding detention

The best way for a Canadian citizen to avoid being detained for extended periods or being sent to a detention center in the United States is to apply for admission through a Canadian Airport that has a preclearance office. U.S. Customs and Border Protection (USCBP) officers at a land port of entry or at inland US airports have the authority to detain foreign nationals for extended periods or even send them to a detention center, because the foreign nationals are already on US soil when they apply for admission. However, the situation is different at a preclearance office located at a Canadian airport.

Foreign nationals who apply for admission through a preclearance office located at a Canadian airport are still in Canada when they apply for admission. USCBP officers located at preclearance offices in Canadian Airports may only exercise the powers that are given to them under the *Preclearance Act, 2016*.[1] Although the *Preclearance Act, 2016* gives USCBP officers greater powers than they had under the prior *Preclearance Act*,[2] it is still more limited than the powers that they possess at a land port of entry or at an inland US airport.

The *Preclearance Act, 2016* currently gives USCBP officers the following powers (among others):

- Under the prior *Preclearance Act*, if a traveller decided to withdraw their application for admission, USCBP officers had no authority to hinder their departure. Under the *Preclearance Act, 2016*, even after the traveller has confirmed their intention to withdraw their application for admission, they must still truthfully answer any questions asked by the USCBP officer for the purpose of identifying the traveller or determining their reason for withdrawing.[3] So, theoretically, a USCBP officer could prevent the traveller from leaving the preclearance area until they have answered these questions to the officer's satisfaction. Fortunately, USCBP officers may only exercise their powers to the extent that doing so would not "unreasonably delay the traveller's withdrawal."

- A USCBP officer may detain a traveller (or their goods) in the preclearance area if they have reasonable grounds to believe that a person has committed an offense under an Act of Parliament.[4] However, they must, as soon as feasible, deliver that person or goods into the custody of a police officer or Canada Border Services Agency (CBSA) officer.[5]

- A USCBP officer may, for the purpose of a strip search, detain a traveller bound for the United States if the officer has reasonable grounds to suspect that:

    - The traveller has on their person concealed goods or anything that would present a danger to human life or safety; and

    - The search is necessary for the purpose of conducting preclearance.[6]

    On detaining a traveller for the purpose of a strip search, the USCBP officer must immediately request that a CBSA officer conduct the search.[7] However, the USCBP officer may conduct the strip search if a

[1] S.C. 2017, c. 27.
[2] S.C. 1999, c. 20.
[3] *Preclearance Act, 2016*, s. 30.
[4] *Id.*, ss. 14(1)(a).
[5] *Id.*, ss.14(1)(2).
[6] *Id.*, ss. 22(1).
[7] *Id.*, ss. 22(2)

CBSA officer refuses to conduct the search or if no CBSA officer is able to conduct the search within a reasonable time.[8]

- A USCBP officer may detain a traveller in the preclearance area if they have reasonable grounds to believe that a traveller bound for the United States poses a risk of significant harm to public health.[9] However, they must, as soon as feasible, deliver the traveller into the custody of a police officer, CBSA officer, or quarantine officer.[10]

The *Preclearance Act, 2016* also creates the following criminal offenses:

- Making an oral or written statement to a USCBP officer with respect to the preclearance of a person or any goods, that the person knows to be false or deceptive or to contain information that the person knows to be false or deceptive is guilty of an offense punishable on summary conviction and is liable to a fine of $5,000.00.[11]

- Resisting or willfully obstructing a USCBP officer at preclearance in the exercise of the officer's powers or performance of their duties and functions, or a person lawfully acting in aid of such an officer is guilty of either an indictable offense (punishable by imprisonment for a term of not more than two years) or an offense punishable on summary conviction.[12]

Theoretically, a USCBP officer could allege that the traveller has made a false/deceptive statement or resisted/obstructed the performance of their duties and functions and then detain the traveller until they can be delivered to a police officer (who may or may not decide to lay charges against that traveller). Even the threat of doing so may cause some travellers to feel that they are not free to leave the preclearance area.

Nevertheless, USCBP officers at preclearance offices in Canadian airports still do not have the same powers that they have when they are on US soil. The *Preclearance Act, 2016,* makes clear that a USCBP officer at a preclearance office is not permitted to "exercise any powers of questioning or interrogation, examination, search, seizure, forfeiture, detention or arrest that are conferred under the laws of the United States."

It should be mentioned that not all flights departing from Canadian airports will preclear, even if there is a preclearance office located at that airport. For example, travellers flying on private jets typically do not preclear at Canadian airports. In addition, although most Canadian international airports have preclearance offices, some do not. Billy Bishop Airport on Toronto Island is a notable exception, although a preclearance office is expected to open at that airport some time in 2025.

Avoiding expedited removal

Expedited removal appears in §235(b)(1) of the *Immigration and Nationality Act* (INA). It was added to the INA in 1996, as a result of the *Illegal Immigration Reform and Immigrant Responsibility Act of 1996*. INA §235(b)(1) allows USCBP officers to order the summary removal of certain foreign nationals from the United States without a hearing or right of appeal. An expedited removal order results in a five-year bar.

Expedited removal may only be ordered when USCBP has found a foreign national to be inadmissible under one of the following grounds of inadmissibility:

- INA §212(a)(6)(C), which relates to fraud, willful misrepresentation, or false claims of US citizenship; or

[8] *Id.*, ss. 22(4).
[9] *Id.*, ss. 15(1).
[10] *Id.*, ss. 15(2).
[11] *Id.*, ss. 37.
[12] *Id.*, ss. 38.

- INA §212(a)(7), which relates to an immigrant who, at the time of application for admission, is not in possession of a valid entry document, a valid unexpired passport or other suitable travel document, or whose visa was not issued compliance with the law.

Unfortunately, INA §212(a)(7) can apply to a foreign national who is simply ineligible for the classification that they have requested. For example, an applicant for admission as a B-2 visitor for pleasure (i.e., tourist) who is denied admission because USCBP believes that they are not a *bona fide* visitor will be inadmissible under INA §212(a)(7). In addition, a TN applicant who is refused at the border, based on the documents that they have presented, will be inadmissible under INA §212(a)(7). In other words, USCBP officers have the authority to impose expedited removal on foreign nationals in a variety of situations.

Fortunately, USCBP officers may not impose expedited removal orders at a preclearance office located in a Canadian airport because it applies to an "arriving alien." This term is defined in 8 CFR §1.1(q) to mean "an applicant for admission coming or attempting to come into the United States at a port of entry." Preclearance offices are not considered ports of entry, so expedited removal does not apply at a preclearance office located in a Canadian airport.

In summary, applying for admission to the United States through a preclearance office located in a Canadian airport should allow travellers to avoid the possibility of expedited removal.

Dealing with border searches of electronic devices

Background

USCBP's current position is that they have the right to search any computer, smartphone or other electronic device when a traveller is applying for admission to the United States. However, the issue is somewhat complicated.

In 1985, the United States Supreme Court found that a routine search of any persons seeking admission to the United States (and their personal effects) may be performed without reasonable suspicion, probable cause or a warrant. [13] The decision was based on the premise that there is a reduced expectation of privacy associated with international travel.[14] However, it predates the ubiquitous adoption of computers, smartphones and other personal electronics devices, which travellers bring with them when they cross the border.

Privacy advocates believe that USCBP's authority to search a traveller's electronic devices should not be applied in the same manner as a briefcase or suitcase. This is because hand-carried electronic devices now have the capacity to store a very large amount of personal or business information. A search of an electronic device gives rise to significant privacy concerns, due to the vast amount of information saved on such devices.

The 2014 United States Supreme Court decision in *Riley* v. *California* appears to support this belief.[15] In that decision, the Court held that, given the significant and unprecedented privacy interests that people have in their digital data, the police could not conduct warrantless searches of the cell phones of people who they arrest. However, the United States Government does not believe that *Riley v. California* applies in the border context.

On Sept. 13, 2017, the Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU) filed a lawsuit against the United States Government on behalf of 11 travellers (10 US citizens and one lawful permanent resident) whose smartphones and other electronic devices were searched without a warrant at the United States border.[16] The lawsuit alleged that *Riley* v. *California* also applied to border searches of electronic devices.

---

[13] *United States* v. *Montoya de Hernandes*, 473 U.S. 531 (1985).
[14] *United States* v. *Flores-Montano*, 541 U.S. 149 (2004).
[15] 573 U.S. 373 (2014).
[16] *Merchant* v. *Mayorkas* (formerly *Alasaad* v. *Wolf*).

The case was filed in the US District Court for the District of Massachusetts. In November 2019, the district court ruled that USCBP could only search a traveller's electronic device if they had reasonable suspicion that the device contained digital contraband. However, the US Court of Appeals for the First Circuit reversed the decision in February 2021. On April 23, 2021, the EFF and the ACLU petitioned the Supreme Court to hear the case. As the case is ongoing, this issue is far from resolved.

USCBP's policy on border searches

On January 4, 2018, USCBP updated its official policy on border searches of electronic devices. CBP Directive No. 3340-049A (the Border Search Directive) addressed some, but not all, of the issues that arise from border searches of electronic devices. Even though it is seven years old, the Border Search Directive is still in force; it is currently referenced on the USCBP website.

Basic v. Forensic Searches

The Border Search Directive makes a distinction between basic and advanced searches:

- An "advanced search" is defined as "any search in which an officer connects 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." Where a USCBP officer has a reasonable suspicion of an activity that violates laws enforced or administered by USCBP or a national security concern, they may perform an advanced search of an electronic device (with supervisory approval).

- A "basic search" is defined as "any border search of an electronic device that is not an advanced search." In the course of a basic search, a USCBP officer may, without having any specific suspicion, examine an electronic device and may review and analyze information encountered during the examination. This includes information that is resident on the device and would ordinarily be visible by scrolling through the phone manually (including contact lists, call logs, calendar entries, text messages, pictures, videos and audio files).

This is essentially a formal recognition of the Federal Court of Appeals decision in *United States* v. *Cotterman*.[17] In that decision, the Ninth Circuit confirmed that USCBP officers needed reasonable suspicion of criminal activity before they could justify a forensic search of a laptop seized at the border. This case was only binding in the Ninth Circuit (Alaska, Hawaii, Washington, Oregon, California, Arizona, Nevada, Montana and Idaho). However, by incorporating the decision into the Border Search Directive, USCBP has confirmed that *United States* v. *Cotterman* applies to all USCBP inspections.

Passcode protected or encrypted information

The Border Search Directive states that a USCBP officer *may* request the traveller's assistance in presenting electronic devices and information contained therein, in a condition that allows inspection of the device and its contents. This appears to suggest that travellers have the option of refusing to unlock their electronic devices. However, the Border Search Directive also states that travellers are "obligated to present electronic devices and the information contained therein in a condition that allows inspection of the device and its contents." So, USCBP clearly believes that travellers must cooperate and give them access to their passcode-protected electronic devices.

If a USCBP officer is unable to complete an inspection of an electronic device because it is protected by a passcode or encryption, the officer may detain the device pending a determination as to its admissibility, exclusion or other disposition. The Border Search Directive makes clear that it does not limit USCBP's ability to seek technical assistance, to use external equipment or to take other reasonable measures to render a device in a condition that allows for inspection of the device and its contents. However, supervisory approval is required in

[17] 709 F.3d 952 (9th Cir. 2013).

order to detain an electronic device or copies of information contained therein, beyond an individual's departure from the port.

A USCBP officer may detain an electronic device or copies of information contained therein, for a "brief, reasonable period of time" to perform a thorough border search "as expeditiously as possible." Unless "extenuating circumstances" exist, the detention of devices ordinarily should not exceed five days. However, nothing precludes USCBP from detaining an electronic device for a much longer period by asserting that "extenuating circumstances" exist.

Although the issue of warrantless border searches of electronic devices is not yet settled, if the traveller is nonimmigrant (i.e., a worker, student or visitor), refusing to unlock their device can have undesirable consequences. For example, USCBP could decide to deny the traveller's application for admission to the United States.

Accessing information saved in the cloud

The Border Search Directive defines the scope of the information that USCBP officers are permitted to access when conducting border searches of electronic devices. It clarifies that a border search should include an examination of only the information that is resident on the device itself and accessible through the device's operating systems or through other software, tools, or applications. In other words, officers may not use the device to access information that is solely stored in the cloud.

Prior to beginning a search, USCBP must take steps to ensure that the electronic device is not connected to any network. In order to avoid accidentally retrieving or accessing information stored in the cloud, which is not otherwise present on the device, USCBP officers must either request that the traveller disable connectivity to any network (i.e., place it in "airplane mode") or in certain cases, disable the network connectivity themselves.

This means that information stored on cloud-based servers (e.g., Dropbox, Google Drive, etc.) should fall outside the scope of a USCBP search. Of course, many applications store local copies of some cloud-based information on the device itself. If this information remains accessible after the device has been disconnected from the Internet, USCBP may examine it.

Privileged and other sensitive information

The Border Search Directive clarifies the specific procedure that USCBP officers must follow when they encounter information that they identify as privileged or over which a claim of privilege has been asserted:

- If a USCBP officer encounters information identified as or asserted to be, lawyer-client privileged information or lawyer work product, the officer must seek clarification from the individual asserting the privilege regarding the specific files, the lawyer or other client names or other particulars that may assist USCBP in identifying the privileged information.

- Prior to any border search of the files or other materials over which privilege has been asserted, the officer must contact the USCBP Associate/Assistant Chief Counsel Office. In coordination with that office, the USCBP officer will ensure the segregation of any privileged material from other information examined during the border search to ensure that any privileged information is handled appropriately. The segregation process will occur through the establishment of a Filter Team composed of legal and operational representatives or through another appropriate measure with written concurrence of the USCBP Associate/Assistant Chief Counsel Office.

- At the completion of the USCBP review, unless materials are identified that indicate an imminent threat to homeland security, copies of materials maintained by USCBP and determined to be privileged will be destroyed, except for any copy maintained solely for the purposes of complying with a litigation hold or other requirement of law.

- Information determined to be protected by law as privileged or sensitive will only be shared with agencies or entities that have mechanisms in place to protect such information.

The Border Search Directive states that other possibly sensitive information (such as medical records and work-related information carried by journalists) will be handled in accordance with any applicable federal law and USCBP policy. It also confirms that USCBP officers encountering business or commercial information on electronic devices must treat it as business confidential information and protect it from unauthorized disclosure.

Although the Border Search Directive establishes a process for information/documentation that is subject to lawyer-client privilege to be segregated from other non-protected information, it requires coordination with the USCBP Associate/Assistant Chief Counsel Office and the actual segregation of privileged information/documentation will typically be done by a team established for this purpose. If privilege is claimed, it appears very likely that USCBP will detain the electronic device until the privileged information/documentation can be identified and segregated from other non-privileged information/documentation; this could take a long time. More importantly, the reference to information determined to be protected by law as privileged "being shared with agencies or entities that have mechanisms in place to protect such information" suggests that even privileged information can be examined and shared with other agencies or entities.

In addition, the Border Search Directive only states that other confidential business or personal information, which is not subject to lawyer-client privilege, will be handled "in accordance with any federal law and USCBP policy." In other words, this confidential information can still be examined as long as it is carried out in compliance with existing federal law.

Safeguarding your digital data

USCBP clearly believes that it has the right to examine a traveller's electronic devices and that travellers are required to present their electronic devices in a condition that allows inspection of the device and its contents (i.e., they are required to unlock their devices). Although this position is still being challenged in the courts, the outcome is uncertain. As a result, nonimmigrants (i.e., workers, students and visitors) who apply for admission to the United States may not be in a position to refuse a warrantless border search of their electronic devices.

A US citizen who refuses a border search of their electronic device cannot be refused admission to the United States, although their electronic device may be detained. However, nonimmigrants are in a far more precarious position. Refusing to cooperate with a border search of their electronic device could prompt USCBP to deny that nonimmigrant's application for admission to the United States. If this occurs, detention, expedited removal and/or other undesirable consequences could theoretically follow as well.

Unfortunately, there is also a very real risk that a nonimmigrant may be denied entry and/or removed from the United States because of photos, videos or even social media posts found on their electronic devices (or online), which are considered adverse to the United States. For example, a French scientist was apparently denied entry to the United States after USCBP officers searched his phone and found messages in which he expressed criticism of the Trump Administration. In another recent case, Dr. Rasha Alawieh, a Lebanese doctor, was removed from the United States after the USCBP officers at Logan International Airport found photos of Hassan Nasrallah (the longtime leader of Hezbollah) on her smartphone.

As Dr. Alawieh apparently deleted the photos from her device before her return trip to the United States, it appears likely that USCBP performed an advanced (forensic) search on her electronic device. According to the Border Search Directive, advanced searches may only be performed if there is reasonable suspicion of an activity that violates laws enforced or administered by USCBP or a national security concern. Although this language is somewhat vague, especially the reference to "national security concern," most Canadians should not be subjected to an advanced search of their electronic devices. Of course, if an advanced search is performed, USCBP may be able to access even deleted files on the electronic device.

Based on the above, Canadians (and other nonimmigrants) travelling to the United States may wish to consider the following:

- They should consider whether they really need to bring their electronic devices with them when they cross the border. If not, the devices should be left behind.

- They should consider not keeping any privileged or confidential business information on their electronic device when they cross the border. Although information/documentation that is subject to lawyer-client privilege is given greater protection under the Border Search Directive, it is likely that the electronic device will be detained for an extended period while USCBP segregates the privileged information from the non-privileged information. In addition, even privileged information may be examined and shared with agencies or entities "that have mechanisms in place to protect such information." Confidential business information is given much less protection than privileged information.

- Any information/documentation that the traveller feels should be kept private should be uploaded to the cloud and deleted from their electronic device. The Border Search Directive makes clear that border searches of electronic devices are limited to what is physically on the device. USCBP officers will direct travellers to set their electronic devices to "airplane mode" before turning the devices over for examination.

- It is important to remember that email clients and other apps save information locally on the device. Before applying for admission to the United States, travellers should set their electronic devices to "airplane mode" and then review these apps to ensure that they do not contain any private/confidential information. They should also check any images or videos stored locally on the device. If it can still be seen while the electronic device is set to "airplane mode," it is physically on the device and USCBP may examine it.

- Of course, taking the above precautions will not necessarily prevent USCBP from accessing deleted files on the electronic device if an advanced search is performed. However, as mentioned above, most Canadians should only be subjected to a basic search.

- Deleting essential apps such as email apps from electronic devices is generally not recommended. A smartphone or computer without an email app may look suspicious to a USCBP officer, since it is rare for someone not to have such an app on their electronic device. This could cause a USCBP officer to suspect that the traveller is hiding something relevant to their inspection.

- Some immigration lawyers have suggested that travellers bring a "burner phone," instead of their actual phone, when they travel to the United States. However, this strategy is also not without risk. Although using a burner phone makes it less likely that USCBP will find potentially harmful information/documentation on their electronic device, even if an advanced search is performed, the mere fact that the traveller is using a burner phone can look suspicious. Burner phones have traditionally been used by criminals to avoid being detected by law enforcement. Although there are legitimate reasons why a law-abiding person might wish to use a burner phone, USCBP may believe that the traveller is attempting to hide something relevant to their inspection.

- Although USCBP officers cannot require travellers to give them access to their cloud-based accounts, including social media accounts, they can still search online for public social media posts. So, travellers may wish to review their social media accounts and confirm that their social posts are not set to "public" or if they are, that they do not contain any controversial statements.

Compliance with the alien registration requirement

Canadians should also be aware of the alien registration requirement, which comes into effect on April 11, 2025.

On January 20, 2025, President Trump issued Executive Order 14159 (*Protecting the American People Against Invasion*). Among other things, it directed the US Department of Homeland Security (DHS) to ensure that aliens comply with their duty to register under INA §262 and ensure that failure to comply is treated as a civil and criminal enforcement priority.

Subject to limited exceptions, the alien registration requirement applies to the following individuals:

- Aliens 14 years of age or older who intend to remain in the US for 30 days or longer must apply for registration and be fingerprinted before the expiration of those 30 days.
- Parents and legal guardians of children below the age of 14 who will remain in the US for 30 days or longer must ensure that these children are registered before the expiration of those 30 days.
- Within 30 days of reaching their 14th birthday, an alien child must apply in person for registration and be fingerprinted.

In addition, according to 8 USC §1305, any foreign national who is subject to registration under the INA (including those who are already registered through their receipt of a Form I-94) and who is in the US must also notify DHS in writing of each change of address within 10 days from the date of such change.

The alien registration requirement and the change of address requirement are discussed in detail, in a previously published article on the subject.

For more information on this topic, please contact the author, Henry J. Chang.