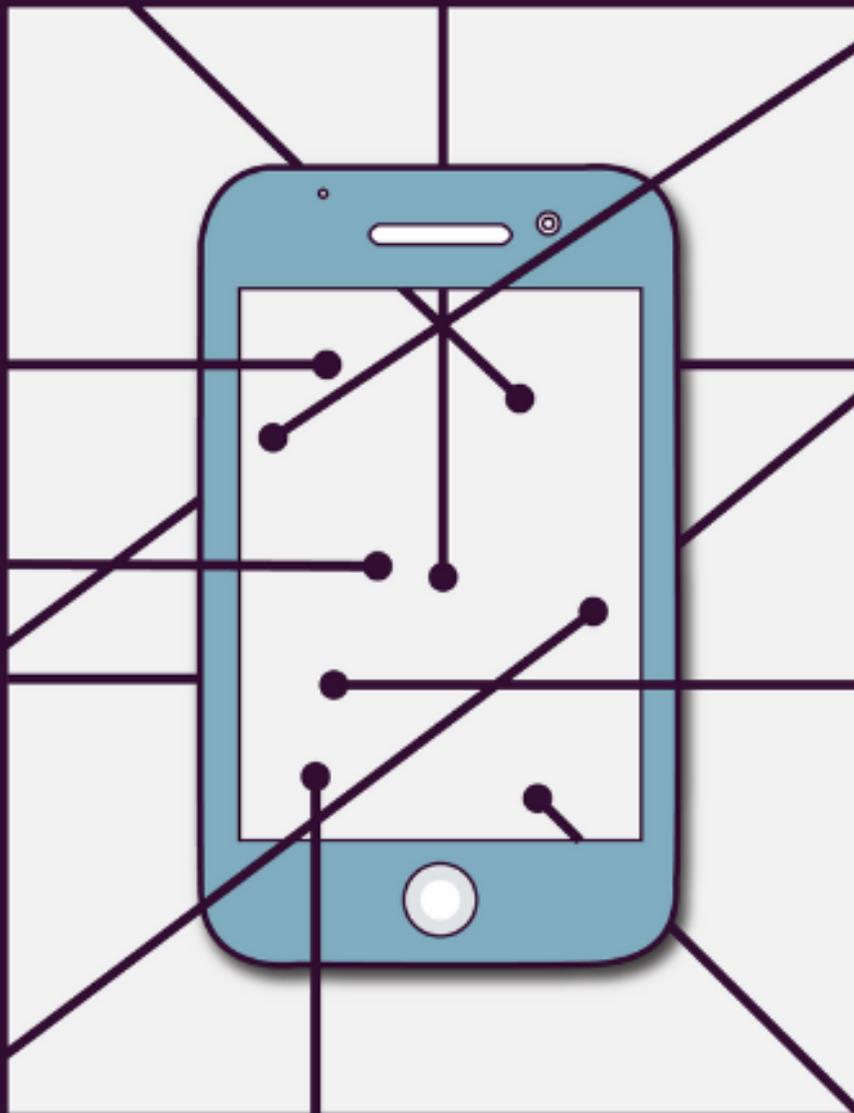


Version abrégée sur les appareils électroniques

*Droits de la protection des
renseignements personnels
numériques à la frontière*



Version abrégée sur les appareils électroniques

Droits de la protection des renseignements personnels numériques à la frontière

Ce guide vous offre de l'information au sujet de vos droits de la protection des renseignements personnels en rapport à vos appareils tels que cellulaires, ordinateurs portatifs et tablettes à la frontière. Il est conçu pour les personnes qui franchissent la frontière pour entrer au Canada ou celles qui quittent pour les É.-U. par les zones de dédouanement préalable au Canada.

Généralement, la police ne peut effectuer de fouilles aléatoires sans soupçon, mais ce n'est pas le cas à la frontière. La *Charte des droits et libertés* s'applique à la frontière, mais les tribunaux ont découvert que l'intérêt du gouvernement d'empêcher les biens dangereux et les personnes indésirables d'entrer au pays confère à l'Agence des services frontaliers du Canada plus de pouvoirs pour fouiller les gens et leurs possessions que les policiers dans d'autres circonstances.

La Loi sur les douanes octroie à l'Agence des services frontaliers du Canada (ASFC) de larges pouvoirs pour fouiller les personnes et les biens qui entrent au pays, incluant les choses que les gens apportent. Ceci inclut le contenu (fichiers, photos et vidéos) de vos appareils numériques. Les fichiers dans vos appareils numériques sont des « biens » en vertu de la Loi sur les douanes et les agents des douanes peuvent fouiller les biens entrant au Canada sans mandat, même s'ils n'ont aucune raison de soupçonner que les biens sont des marchandises de contrebande ou en contiennent.

Les non-citoyens qui désirent entrer au Canada, incluant les demandeurs d'asile, peuvent aussi être soumis à des fouilles. En vertu de la Loi sur l'immigration et la protection des réfugiés, un agent de l'ASFC peut fouiller les bagages et les effets personnels d'une personne qui demande l'entrée au Canada à un point d'entrée, incluant les appareils et les supports électroniques. Toutefois, l'agent doit avoir :

- des motifs raisonnables de croire que la personne n'a pas révélé son identité ou a caché sur sa personne des documents pertinents à son admissibilité, ou
- des motifs raisonnables de croire que la personne est impliquée avec des gens qui font de la contrebande, la traite des personnes ou la fraude de documents.

Les fouilles d'appareils doivent se limiter à identifier la personne, trouver des documents pertinents à l'admissibilité ou des preuves des infractions susmentionnées.

Fouilles initiales

Les agents de première ligne effectuent les fouilles initiales du contenu de vos appareils en parcourant les images, vidéos et fichiers. Il devrait s'agir d'un regard sommaire du contenu dans le but de déterminer s'il contient de la contrebande comme de la pornographie juvénile ou de la littérature haineuse ou des preuves d'un crime. Les fouilles initiales peuvent être aléatoires ou ciblées.

Quiconque peut faire l'objet d'une fouille aléatoire. On craint que les voyageurs soient ciblés pour des fouilles en fonction de leur race ou de leur religion et qu'un tel profilage puisse être présenté comme une fouille « aléatoire ». Bien que ce genre de profilage serait une infraction, la discrimination est très difficile à prouver. Si vous croyez avoir été victime de discrimination, de plus amples renseignements sur la manière de porter plainte sont inclus ci-dessous.

La plupart des gens fouillés par l'ASFC ne sont pas choisis au hasard, mais ils sont plutôt ciblés. Les gens sont ciblés en fonction de renseignements provenant des bases de données sur les voyageurs, particulièrement pour les arrivées par avions, trains ou bateaux de croisière, ainsi que des « indicateurs »

qui, selon l'Agence, augmentent la probabilité que les appareils électroniques de la personne contiennent une forme de contrebande. Il n'existe aucune liste disponible publiquement des indicateurs utilisés par l'Agence, mais il est à noter que vous êtes plus susceptible de faire l'objet d'une fouille si :

- vous importez quelque chose que l'ASFC juge suspect, ou si vous êtes associé à des importateurs ou exportateurs connus de matières auxquelles l'Agence s'objecte; vous avez en votre possession des animés et des mangas, pour lesquels l'Agence a beaucoup de soupçons;
- vous avez voyagé vers des destinations à risques élevés (bien qu'aucune liste ne soit disponible, ces destinations incluent sans doute l'Asie du Sud-Est, l'Allemagne, Cuba et l'Espagne);
- vous êtes un homme célibataire qui voyage seul;
- vous semblez nerveux, agité;
- vous avez en votre possession de multiples appareils électroniques (incluant des disques durs);
- vous démontrez un intérêt pour la pornographie, comme l'indiquent les noms de fichiers et de dossiers dans votre appareil;
- vous avez acheté un billet pour voyager à la dernière minute;
- un code sur votre valise ne correspond pas à l'endroit d'où vous provenez;
- vos itinéraires de voyage sont inhabituels.

Durant une fouille initiale, les agents ne devraient pas lire attentivement tous les documents ni examiner les photos dans votre appareil. Ils devraient seulement regarder le contenu assez longtemps afin de déterminer qu'il n'inclut pas de contrebande (comme de la pornographie juvénile) ou de confirmer ou dénier les soupçons au sujet d'une infraction aux lois des douanes ou de l'immigration. L'information obtenue durant une fouille initiale peut être utilisée pour justifier une recherche plus approfondie.

Les agents devraient simplement regarder le contenu qui est déjà sur l'appareil. Ils doivent mettre l'appareil en mode « avion » et regarder seulement le contenu local (y compris les courriels et textos marqués comme « lus »). L'ASFC affirme qu'elle obtient un mandat d'un juge pour fouiller les renseignements accessibles seulement à distance. Toutefois, on sait que l'ASFC demande parfois au voyageur d'ouvrir volontairement une session d'un compte à distance; les voyageurs ne peuvent donc pas s'attendre catégoriquement à ce que les comptes de médias sociaux liés restent privés lorsqu'ils franchissent la frontière.

Fouilles détaillées

Si un agent trouve quelque chose qui, selon lui, mérite une inspection plus attentive, une fouille plus approfondie peut être effectuée. Ces fouilles peuvent être faites par des spécialistes ayant de l'expérience dans l'utilisation d'outils d'analyse.

Lors d'une fouille approfondie, votre appareil vous sera retiré. La Loi sur les douanes octroie à l'ASFC le pouvoir de retenir des biens si un agent n'est pas satisfait qu'ils aient été convenablement inspectés aux fins d'admission au Canada. Les agents peuvent aussi copier l'intégralité du contenu de votre appareil. Ceci permet à l'ASFC d'utiliser ultérieurement un logiciel de décodage de mots de passe pour accéder au contenu pour lequel vous n'avez pas fourni de mot de passe.

Selon l'ASFC, des copies des données ne sont pas retenues après l'enquête. Toutefois, nous savons que l'ASFC peut partager vos renseignements personnels qu'elle recueille lors des enquêtes avec d'autres agences gouvernementales comme la GRC et les agences de sécurité comme le Service canadien du renseignement de sécurité (qui peut à son tour les partager avec des gouvernements étrangers à des fins de renseignement).

Mots de passe

Les agents peuvent vous demander votre mot de passe ou empreinte pour accéder aux renseignements stockés dans votre appareil. Il y a incertitude quant à la question de savoir si vous êtes légalement tenu de le fournir, bien que l'ASFC ait pu arrêter ou menacer d'arrêter des gens à défaut de fournir le mot de passe. L'ASFC soutient qu'elle a le droit d'arrêter les personnes qui ne fournissent pas de mots de passe et qu'elle peut le faire si l'agent a une bonne raison de croire que l'appareil contient du matériel interdit.

La position de l'ASFC en 2017 était qu'elle ne peut contraindre quelqu'un à fournir des mots de passe pour obtenir l'accès à tout compte, fichier ou information stocké à distance. Si on vous demande un mot de passe pour accéder à un compte en ligne, vous ne devriez faire face à aucune conséquence pour refuser de le fournir.

Si on vous demande et que vous choisissez de ne pas divulguer votre mot de passe ou de fournir une empreinte pour accéder à l'information stockée dans votre appareil, vous risquez d'augmenter les soupçons de l'ASFC au sujet du contenu de votre appareil, de vous voir refuser l'entrée si vous n'êtes pas citoyen canadien ou résident permanent, la détention ou la saisie de votre appareil pour une inspection plus approfondie par des spécialistes judiciaires (ce qui pourrait prendre des mois), ou l'arrestation. Entraver le travail d'un agent de l'ASFC est une infraction passible d'amendes pouvant atteindre 50 000 \$ et d'une peine d'emprisonnement de cinq ans.

Zones américaines de prédédouanement au Canada

Les agents de la U.S. Customs and Border Patrol sont autorisés à appliquer les lois américaines dans des parties des aéroports, gares ferroviaires et gares maritimes au Canada où des voyageurs en partance vers les É.-U. peuvent passer à la douane américaine avant de quitter le Canada. Dans ces secteurs, l'application des lois américaines est soumise aux lois canadiennes des droits de la personne, incluant la *Charte des droits et libertés*. Les normes canadiennes en matière de fouilles et de saisies sont donc celles qui s'appliquent, et non les normes américaines. Toutefois, il y a incertitude quant à la question de savoir si les agents connaissent les normes juridiques appropriées et s'ils ont reçu de la formation à leur sujet.

En ce qui concerne les fouilles d'appareils électroniques, les lois américaines sont semblables aux lois canadiennes : les agents n'ont pas besoin de mandat ni même d'un soupçon raisonnable pour regarder votre téléphone. Il devrait s'agir du contenu local seulement, rien qui exige une connexion à un réseau pour être affiché.

Les agents des douanes américaines effectuent des fouilles de base et avancées. Les fouilles de base peuvent être effectuées avec ou sans soupçon et incluent toute fouille d'un appareil électronique qui ne constitue pas une fouille approfondie.

Dans le cas d'une fouille approfondie, l'appareil est branché à une pièce d'équipement externe afin d'avoir accès au contenu et aussi possiblement d'en faire une copie. Des fouilles approfondies exigent un soupçon raisonnable d'une infraction aux lois américaines ou d'une préoccupation en matière de sécurité nationale.

Les agents des douanes américaines peuvent vous demander votre mot de passe. Si vous ne le fournissez pas, l'agent peut refuser de vous laisser franchir les douanes en vue de votre départ vers les É.-U. L'agent peut aussi détenir votre appareil afin qu'une fouille plus approfondie soit effectuée. Votre appareil ne

devrait pas être détenu plus de cinq jours, mais des rapports indiquent que les appareils sont parfois conservés pendant plusieurs mois.

Conseils

Compte tenu des mesures que vous prenez pour protéger vos renseignements confidentiels, sachez que votre interaction avec un agent frontalier pourrait s'intensifier s'il détecte que vous avez tenté délibérément d'entraver une fouille, particulièrement d'une manière qui détruit des données auxquelles vous auriez pu avoir accès autrement, ou si vous avez dissimulé le fait que les données étaient présentes.

- **Laissez vos appareils à la maison** si vous n'en avez pas besoin en voyage ou **utilisez un appareil exclusivement pour le voyage** qui ne contient aucune donnée ni activité.
- **Effectuez une copie de sauvegarde** de vos données avant de franchir la frontière et laissez-la à la maison. Ceci est important si votre appareil est détenu ou saisi, mais permet également de supprimer toute donnée inutile dans votre appareil avant de franchir. Vous pouvez également effacer tout le contenu de votre appareil avant de franchir la frontière et le restaurer par la suite à partir de la copie de sauvegarde.
- **Supprimez définitivement les données** dont vous n'avez pas besoin en voyage. Il ne s'agit pas de simplement les mettre dans le bac de recyclage. Il faut utiliser les outils intégrés dans Windows (un outil nommé *cipher*), Mac ('*vider la corbeille en mode sécurisé*') ou Linux (*déchiqueter* ou *vider la corbeille en mode sécurité*) afin de supprimer les données en permanence. Il est à noter que les agences frontalières ont accès à des outils d'analyse sophistiqués et peuvent voir des renseignements au sujet des données supprimées qu'une personne moyenne ne peut pas. Appuyer sur « supprimer » ne garantit pas qu'un agent frontalier sera incapable de trouver l'information.
- **Utilisez un mot de passe** pour ouvrir une session ou avoir accès à votre appareil. Un agent qui est seulement légèrement curieux et allume votre appareil électronique dans le but de jeter un coup d'oeil au contenu pourrait perdre l'intérêt en réalisant qu'il devra vous demander votre mot de passe.
- **Créez un mot de passe sécurisé** en utilisant par exemple plusieurs mots aléatoires (une 'phrase passe') si possible, en évitant des mots de passe faciles à deviner.
- **Éteignez votre ordinateur** avant de passer à la douane et assurez-vous qu'aucun compte ou application n'est réglé en mode d'ouverture de session automatique lors de l'activation.
- **Utilisez une authentification à deux facteurs**, au cas où l'agence frontalière saisisse un appareil et non l'autre.
- **Utilisez le chiffrement complet de disque** et exigez une phrase passe forte pour y accéder. De nombreux appareils incluent cette option. Ceci peut protéger vos données, même contre les analystes les plus expérimentés. Toutefois, ce qui se produira n'est pas très clair si votre appareil électronique est détenu et que l'agence frontalière est incapable d'accéder aux données. Votre appareil pourrait être saisi et jamais retourné.
- Si vous choisissez de ne pas utiliser un chiffrement complet de disque, vous pouvez aussi chiffrer des **documents ou fichiers critiques précis** à l'aide du logiciel intégré.
- Séparez les documents protégés par le secret professionnel et confidentiels dans leur propre dossier afin qu'il soit clair qu'ils sont protégés. Ceci inclut les fichiers d'avocats et parfois les fichiers de médecins, psychologues, psychiatres et journalistes. Les agents frontaliers sont censés prendre des précautions pour ne pas regarder des documents protégés par le secret professionnel

lorsqu'ils sont avertis de leur existence, sauf pour vérifier qu'ils le sont bel et bien. En théorie, ils ne devraient regarder aucun fichier protégé par le secret professionnel, mais il est possible que les agents frontaliers ne respectent pas la loi dans ce domaine.

Déposer une plainte

Si vous pensez que votre fouille était abusive, mais que votre plainte n'est pas en rapport à une discrimination ou une atteinte à la vie privée, vous pouvez porter plainte directement à l'Agence des services frontaliers du Canada. Si votre appareil a été saisi ou si vous avez reçu une pénalité ou une amende, vous pouvez faire une [demande de révision de la décision](#).

Vous pouvez également envoyer des commentaires écrits à la [Direction des recours](#) de l'ASFC qui examine la conduite des agents. Assurez-vous d'inclure tous les renseignements pertinents afin que l'agent des recours comprenne votre plainte et communique avec vous.

Si vous croyez avoir été victime de discrimination de la part d'un agent de l'ASFC, vous pourriez être en mesure de déposer une plainte à la [Commission canadienne des droits de la personne](#). Les motifs de discrimination incluent la race, l'origine nationale ou ethnique, la couleur, la religion, l'âge, l'orientation sexuelle, l'identité ou l'expression sexuelle, l'état matrimonial, l'état civil, une incapacité, des caractéristiques génétiques ou une condamnation pour laquelle un pardon a été accordé ou un dossier a été suspendu.

Si vous croyez que l'ASFC a porté atteinte à votre vie privée, vous pouvez peut-être déposer une plainte auprès du [Commissariat à la protection de la vie privée du Canada](#), qui veille au respect de la Loi sur la protection des renseignements personnels par le gouvernement.

Vous pouvez aussi signaler tout incident pertinent à des groupes intéressés de défense des droits civiques au Canada, incluant la [Coalition pour la surveillance internationale des libertés civiles](#) et le [Conseil national des musulmans canadiens](#).

Si vous croyez qu'il y a eu atteinte à votre vie privée ou si vous avez été victime de discrimination de la part d'agents américains dans les zones de prédédouanement, nous vous recommandons d'écrire au [ministre de la Sécurité publique](#) et au [ministre des Affaires étrangères](#). Vous pouvez aussi communiquer avec le [Bureau des droits civils et des libertés publiques](#) au département de la Sécurité intérieure, le [chef de la protection de la vie privée](#) du département de la Sécurité intérieure et le [Traveler Redress Inquiry Program](#) du département de la Sécurité intérieure. Vous pouvez aussi signaler tout incident pertinent à des groupes intéressés de défense des droits civils, incluant la [Electronic Frontier Foundation](#), le [Council on American-Islamic Relations](#) et l'[American Civil Liberties Union](#).



www.bccla.org



@bccla



@BCCivLib



www.cippic.ca



@cippic



BÂTIR UN MEILLEUR
CANADA EN LIGNE

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