CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

ETHI • NUMÉRO 065 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 15 juin 2017

Président

M. Blaine Calkins

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Le jeudi 15 juin 2017

● (1535)

[*Traduction*]

Le président (M. Blaine Calkins (Red Deer—Lacombe, PCC)): Bon après-midi, chers collègues. Je m'excuse pour le léger retard. Nous venons tout juste d'arriver à la salle du comité, qui se situe dans l'un des immeubles les plus éloignés de la Chambre des communes, où nous venons de conclure un vote pour ensuite découvrir que nous devrons retourner à la Chambre des communes pour un autre vote très bientôt.

Je propose d'écouter le plus de témoignages possible de nos témoins.

Merci d'être là aujourd'hui. Nous devrons probablement nous absenter pendant quelques minutes pour retourner voter. Vu le temps que le processus est susceptible de prendre, nous déterminerons à ce moment-là si nous vous demanderons ou non d'attendre patiemment notre retour. Merci de votre patience jusqu'à présent.

Nous accueillons aujourd'hui comme témoin Brenda McPhail de l'Association canadienne des libertés civiles. C'est une habituée des réunions du Comité.

Très heureux de vous voir, Brenda.

Nous accueillons aussi Micheal Vonn, elle aussi une habituée des réunions du Comité, qui est en compagnie de Meghan McDermott, toutes les deux de l'Association des libertés civiles de la Colombie-Britannique, puis nous accueillons finalement Esha Bhandari, avocate-conseil de l'American Civil Liberties Union. Vous comparaissez tous par vidéoconférence, sauf Brenda, que nous avons la chance d'avoir avec nous.

Nous en sommes à la 65e réunion du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique et nous étudions la protection des renseignements personnels des Canadiens aux postes frontaliers, dans les aéroports et voyageant aux États-Unis.

Ce sera une très brève étude, alors, sans plus attendre, je demande à Mme McPhail de commencer. Vous avez jusqu'à 10 minutes.

Mme Brenda McPhail (directrice, Projet sur la confidentialité, la technologie et la surveillance, Association canadienne des libertés civiles): Merci beaucoup au Comité d'avoir invité l'Association canadienne des libertés civiles à discuter de cet important sujet.

L'ACLC, comme vous le savez, est une organisation nationale indépendante et non gouvernementale qui se bat pour les libertés civiles au Canada depuis 1964.

Aujourd'hui, je vais parler de trois sujets, le premier, plus longuement, puis les autres, très rapidement. Le premier, c'est le besoin de mettre à jour les lois et les politiques concernant les fouilles des appareils à la frontière de façon à refléter les attentes plus élevées en matière de protection des renseignements personnels associés à ces appareils. Viendra ensuite l'important besoin de transparence publique et de responsabilisation quant à la façon dont les lois actuelles sont interprétées à la frontière et, plus particulièrement, les politiques et les procédures en place concernant tout particulièrement les fouilles intrusives en ce qui a trait à la vie privée. Je vais ensuite très rapidement parler du besoin de s'assurer que la nouvelle Loi sur le précontrôle, le projet de loi C-23, maintient ou accroît les protections de la vie privée dont bénéficient les Canadiens et les voyageurs en sol canadien plutôt que de les réduire.

Je ne vais pas parler longtemps du décret exécutif du président Trump concernant l'exclusion des citoyens non américains des protections liées à la vie privée au titre de la loi américaine sur la protection de la vie privée, mais je tiens à souligner que l'ACLC a les mêmes préoccupations que celles qu'a formulées le commissaire à la protection de la vie privée dans sa lettre datée du 8 mars, et nous croyons nous aussi que le gouvernement doit demander aux États-Unis d'améliorer la protection en matière de vie privée accordée aux Canadiens au titre de cette loi.

L'étude que vous réalisez arrive à point et est extrêmement nécessaire vu toutes les histoires dont on entend parler, les récits de personnes à qui l'on pose des questions intrusives et humiliantes au sujet de leurs croyances religieuses, de leur origine ethnique, de leur sexualité et de leurs croyances politiques des deux côtés de la frontière, du côté tant canadien qu'américain. Elle s'impose également, à l'inverse, vu toute la rhétorique qu'on entend sur le contrôle extrême qui s'appuie sur une crainte persistante du terrorisme et de « l'autre ».

Je vais surtout parler de la loi, en principe, mais je tiens à souligner d'entrée de jeu que la raison pour laquelle nous devons penser longuement et sérieusement aux façons d'améliorer la protection de la vie privée à la frontière est liée aux coûts pour les personnes et la confiance publique si on ne le fait pas.

L'ACLC gère une ligne d'information, et, sur cette ligne, les questions liées à la frontière ont augmenté de façon majeure au cours des six derniers mois. Nous recevons des appels de musulmans et de chrétiens, d'hommes et de femmes de couleur différente et d'orientation sexuelle différente, et ils craignent tous la même chose. Ils craignent de faire l'objet de fouilles ou de se faire poser des questions envahissantes lorsqu'ils traversent la frontière. Certains ont même peur de voyager.

Nous ne pouvons pas faire grand-chose au sujet de la façon dont les Canadiens sont traités à la frontière américaine, mais nous pouvons et nous devons régler les problèmes qui existent de notre côté. J'irai encore plus loin et je dirai que l'heure est venue pour le Canada d'assumer un rôle de leadership à l'échelle internationale ou en matière de droits lié aux lois, aux politiques et aux pratiques concernant la sécurité à la frontière.

On croit souvent que les frontières sont des zones spéciales où les droits à la vie privée sont réduits en raison du devoir pressant de protéger la souveraineté des États et de la population. Nous ne nions pas ce devoir ni le besoin d'assurer une sécurité efficace à la frontière pour y arriver, mais il ne faut pas oublier que le fait d'avoir des attentes « réduites » en matière de protection de la vie privée ne veut pas dire et ne devrait jamais être synonyme d'« absence » de ces attentes, et, selon nous, pour être vraiment efficace dans le meilleur sens du terme, la sécurité doit trouver un juste équilibre entre la rigueur et le respect des droits.

C'est particulièrement important lorsqu'il est question des fouilles des appareils électroniques, y compris les téléphones cellulaires, les ordinateurs portables et les technologies vestimentaires. Nous vivons dans un monde où les outils que nous utilisons de plus en plus pour vivre au quotidien — parfois à dessein, et, parfois, par défaut — contiennent, créent et réunissent des renseignements sur nous qui sont profondément personnels et de nature délicate. Il faut arrêter d'essayer d'inclure ces technologies dans des structures juridiques et réglementaires créées à une époque où ces appareils et la quantité et la qualité des renseignements qu'ils contiennent étaient inconcevables.

Je sais que le Comité a entendu des variations très similaires sur le même thème dans le cadre de ses études concernant la Loi sur la protection des renseignements personnels et la LPRPDE, et la question est tout aussi pertinente, et le besoin, tout aussi impérieux, dans le cadre de l'étude actuelle.

Selon moi, il est tout à fait possible pour nous de faire mieux. Lorsqu'il est question d'application de la loi à l'extérieur du contexte frontalier, nous commençons en fait, lentement, à déterminer de quelle façon composer avec ces appareils, l'information qu'ils contiennent et le fait que même des bribes d'information qui semblent anodines peuvent avoir des répercussions liées à la protection de la vie privée. Ce sont des travaux qui sont vraiment encore en cours, mais force est d'admettre qu'il y a eu certaines percées. Plus particulièrement, nous avons reconnu que l'atteinte à la vie privée associée aux fouilles d'un appareil électronique exige la mise en place d'un cadre clair en vertu des lois nationales pour s'assurer que les fouilles en tant que telles sont raisonnables, qu'elles sont réalisées de façon raisonnable et que, autrement, elles respectent la Charte, ce dont on peut habituellement s'assurer en exigeant une autorisation judiciaire préalable — un mandat — et lorsqu'il y a des motifs adéquats qui justifient la fouille.

Il n'y a aucune bonne raison pour laquelle nous ne pouvons pas produire des lois claires qui nous permettent de faire la même chose à la frontière, même si on tient compte du contexte unique dans ce cas-là. La pratique actuelle de l'ASFC n'est pas suffisante. Les agents de l'ASFC réalisent sans mandat des fouilles des appareils électroniques sans qu'aucun seuil n'ait été défini en ce qui a trait aux motifs des fouilles. Ces fouilles sont en grande partie fondées sur des interprétations inexpliquées de la législation qui devait à l'origine s'appliquer à des moyens de transport, des voitures, des boîtes et des bagages. En outre, la façon dont les fouilles sont réalisées n'a pas encore fait l'objet d'un examen public ou judiciaire digne de ce nom.

L'information recueillie à partir des appareils fouillés ou confisqués par l'ASFC est récupérée sans qu'on sache publiquement à quoi elle servira, si elle sera conservée ou, dans l'affirmative, pendant combien de temps et si elle sera communiquée, de quelle façon elle le sera et avec qui. Beaucoup de personnes, depuis les membres du milieu des affaires jusqu'à des journalistes en passant par des chercheurs, des médecins et des avocats, ont aussi l'obligation professionnelle de maintenir la confidentialité et l'intégrité de leurs données. La loi actuelle n'est absolument pas en mesure de composer avec cette réalité.

Il y a aussi des contestations constitutionnelles actuellement déposées devant des tribunaux inférieurs liés aux fouilles d'appareils. Même si la tendance jusqu'à présent semble être au règlement pour faire disparaître les poursuites, à un moment donné, il faudra examiner ces questions devant un tribunal. Selon nous, ce devrait être nos législateurs qui s'en occupent. On attend la mise à jour de la Loi sur les douanes depuis trop longtemps. C'est aussi le cas d'autres textes législatifs qui s'appliquent à la frontière. Il faut en effet reconnaître qu'il y a une différence entre un sac rempli de sous-vêtements et un appareil qui contient les conversations les plus intimes et personnelles, les réflexions et affiliations politiques, la croyance religieuse, les registres financiers, les secrets commerciaux, les renseignements sur la santé et beaucoup d'autres types de renseignements et permettent d'y avoir accès.

Il faut aussi reconnaître dans ce contexte que certains groupes — par exemple, les musulmans ou les personnes qu'on croit être des musulmans, ce qui n'est pas toujours la même chose — ont manifestement fait l'objet d'un examen plus soutenu à la frontière, peut-être encore plus depuis le décret présidentiel américain communément appelé l'« interdiction de voyager des musulmans ». Toute mesure donnant aux représentants à la frontière des pouvoirs de réaliser des fouilles invasives ou qui permettent le maintien de l'ambiguïté, de l'incertitude et des pouvoirs discrétionnaires incontrôlés relativement à ces questions risque de toucher de façon disproportionnée les membres de ces groupes.

On ne peut pas non plus parler des fouilles des appareils sans au moins aborder les sujets connexes comme la communication sous contrainte des mots de passe et l'accès forcé aux justificatifs d'identité des médias sociaux. Ces pratiques révèlent vraiment à quel point il est illogique de traiter les dispositifs électroniques comme toute autre marchandise qui traverse la frontière. Même si l'ASFC devrait pouvoir continuer, bien sûr, à confisquer les appareils, à obtenir un mandat et à mener des recherches judiciaires lorsqu'il y a des motifs raisonnables de le faire, les personnes ne devraient pas avoir l'obligation de participer au processus.

Nous avons appris dans un document provisoire de 2015 qui a été publié grâce à une demande d'accès à l'information que l'ASFC croit avoir le pouvoir d'imposer des pénalités aux voyageurs qui refusent de fournir le mot de passe d'un dispositif donné. Selon l'ACLC, du moins, dans certains cas, exiger la communication d'un mot de passe existant seulement dans la tête d'une personne pourrait être contraire aux droits au silence et à celui de ne pas s'auto-incriminer garantis par la Charte. Et cela s'ajoute aux autres droits à la protection de la vie privée qui sont aussi clairement en jeu.

Actuellement, le Canada ne demande pas les mots de passe ou les justificatifs d'identification des médias sociaux qui permettraient d'avoir accès aux données stockées à distance, et il n'y a aucun pouvoir législatif permettant de justifier une telle demande. Nous voulons simplement déconseiller ne serait-ce qu'aller dans cette direction, parce que ce sera inefficace et cela soulèverait de graves questions d'un point de vue constitutionnel.

Les médias sociaux sont un endroit où les gens peuvent jouer avec leur identité et le font, ce qui rend l'information qu'on y trouve profondément non fiable. Nous savons bien sûr — les sciences sociales nous l'apprennent — que les gens qui pensent être regardés changent leur comportement et il y a aussi des répercussions sur le contenu qu'ils estiment pouvoir regarder, examiner, apprendre et étudier. Cela signifie qu'un tel examen pourrait aussi avoir un effet de refroidissement important sur d'autres libertés fondamentales que nous chérissons, y compris la liberté d'association et la liberté d'expression.

Le deuxième sujet que je veux mentionner très brièvement, c'est le besoin d'accroître la transparence publique et la responsabilisation quant à la façon dont nos lois actuelles, y compris la Loi sur les douanes et la Loi sur l'immigration et la protection des réfugiés, sont interprétées à la frontière, surtout en ce qui a trait à la question des fouilles et des questions portant atteinte à la vie privée. J'ai mentionné que nous avons accès à un petit nombre de documents stratégiques. On peut en fait les consulter sur le site Web de notre collègue, l'ALCCB. Cependant, deux ou trois documents que nous avons reçus grâce à une demande d'accès à l'information de 2015 ne satisfont vraiment pas à l'exigence de responsabilisation publique ni de transparence. Nous ne savons même pas si les documents sont complets, exacts ou à jouer. À l'opposé, si nous regardons ce que font nos voisins du Sud, ils ont en fait publié proactivement leur document stratégique lié à ce genre de fouille, une étude de l'incidence sur la vie privée qu'ils ont réalisée et des statistiques concernant les fouilles électroniques qu'ils réalisent. Il n'y a aucune raison pour laquelle nous ne pouvons pas faire la même chose, ici.

Pour une personne ordinaire à la frontière canadienne, c'est difficile, voire impossible, d'évaluer si la façon dont la fouille est réalisée respecte les normes constitutionnelles. En d'autres mots, les gens qui ont peur de qui j'ai parlé au début de mon exposé n'ont aucune façon de savoir si la façon dont on les traite à la frontière est légale et juste s'ils n'ont pas accès aux politiques et aux procédures qui sont censées être respectées. Bien sûr, sans surveillance indépendante de l'ASFC, même si on peut espérer que les choses changeront, c'est extrêmement difficile d'obtenir un recours.

● (1540)

Pour les six secondes qu'il me reste, je vais vous demander de jeter un coup d'oeil au projet de loi C-23 en ce qui concerne ses répercussions sur la vie privée, en particulier à l'égard de la capacité des agents américains d'effectuer des fouilles à nu si un agent canadien refuse de le faire. Cela ouvre un territoire très dangereux. Les frontières requièrent une attention particulière, non pas seulement parce qu'elles sont des zones où nous avons besoin de sécurité, mais également parce qu'elles sont le premier endroit où les gens qui viennent au Canada interagissent avec ce que nous espérons être un pays libre et démocratique. Nous devons leur montrer qui nous sommes en nous assurant que nos politiques et nos lois à la frontière reflètent nos valeurs.

Le président: Merci beaucoup, Brenda.

Nous allons maintenant passer à l'Association des libertés civiles de la Colombie-Britannique.

Micheal, c'est vous qui commencez.

● (1545)

Mme Micheal Vonn (directrice de la politique, Association des libertés civiles de la Colombie-Britannique): Oui.

Je remercie le Comité de m'avoir invitée à participer à cette étude qui tombe à point nommé.

Manifestement, les Canadiens sont de plus en plus préoccupés par la protection de leurs renseignements personnels dans le contexte de la circulation des données entre les frontières et à la frontière. Notre association aide les gens à comprendre leurs droits à la protection de la vie privée. De fait, ce matin même, l'Autorité canadienne pour les enregistrements Internet a annoncé qu'elle finance conjointement notre projet avec la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) pour la production d'un guide relatif à la protection des renseignements personnels et à la sécurité en ce qui concerne les appareils électroniques à la frontière. Nous le faisons parce que les Canadiens ont besoin de conseils fiables et pratiques dans ce domaine, mais ils ont également besoin de mesures de protection appropriées dans les lois et les politiques.

Il existe évidemment un grand nombre de sujets qui pourraient être abordés dans ce contexte, et seuls quelques-uns peuvent l'être au cours d'un exposé. Je veux discuter de la Privacy Act américaine et d'ententes sur l'échange de renseignements, tandis que ma collègue traitera des seuils appropriés en ce qui concerne les fouilles, du nouveau projet de loi sur le précontrôle et du secret professionnel des avocats.

À l'instar de nos collègues de l'ACLC, nous recommandons de tenir compte des préoccupations du Commissariat à la protection de la vie privée du Canada (CPVP) quant à l'ajout du Canada à la liste des pays désignés dont les citoyens sont protégés par la Privacy Act des États-Unis. Comme les responsables l'ont indiqué dans leur lettre du 8 mars aux ministres de la Justice, de la Sécurité publique et de la Défense, le niveau de protection des données pour les Canadiens serait rehaussé pour atteindre celui accordé aux personnes de divers pays européens.

Maintenant, il importe de souligner — et peut-être que notre collègue à l'ACLU s'intéressera à cet aspect — que la Privacy Act des États-Unis n'offre qu'une protection limitée en matière de renseignements personnels, compte tenu d'un grand nombre d'exemptions importantes, notamment celles relatives à l'application de la loi et à la sécurité nationale. Néanmoins, les Canadiens, qui ont compris qu'on leur refuse même ces mesures de protection limitées, contrairement aux personnes d'autres pays, ont raison d'exiger qu'on remédie à la situation.

Le rapport récemment publié de la toute première consultation canadienne sur le cadre de sécurité nationale fournit clairement un contexte important au présent Comité dans son étude. Il est évident que les Canadiens sont très soucieux du respect de leur vie privée et insistent sur le fait que les pouvoirs d'enquête et de collecte de données pour l'application de la loi et la sécurité nationale doivent être manifestement nécessaires, proportionnés et faire l'objet d'une reddition de comptes. Un secret extrêmement problématique a créé une méfiance croissante relativement à la circulation transfrontalière des données et a soulevé une préoccupation liée au tort réel causé aux Canadiens.

Si vous le voulez bien, rappelons-nous une foule de reportages il y a quelques années à peine au sujet de personnes au Canada qui se sont vu refuser l'entrée aux États-Unis en raison de renseignements personnels sur la santé mentale auxquels avaient eu accès les autorités frontalières américaines. Le Bureau du Commissaire à l'information et à la protection de la vie privée de l'Ontario a dû faire enquête pour savoir comment les autorités frontalières des États-Unis avaient trouvé ces renseignements sensibles sur l'état de santé des Canadiens. Le rapport du commissaire à la protection de la vie privée décrit la façon dont ces renseignements ont été enregistrés dans la base de données du Centre d'information de la police canadienne (CIPC) et auxquels le FBI a eu accès grâce à un protocole de coopération avec la GRC. Cette entente permettait au FBI de décider par ailleurs à qui d'autre transmettre ces renseignements, et il a décidé que les entités du département de la Sécurité intérieure, y compris les autorités frontalières, devaient également y avoir accès.

Ce ne sont là que quelques-unes des ramifications de la circulation des renseignements personnels que favorise un simple protocole. Soulignons rapidement, comme je l'ai dit, que, compte tenu des exemptions contenues dans la Privacy Act des États-Unis, nous ne pourrions envisager aucun recours à l'égard de cette circulation des données si nous étions protégés par cette loi.

L'important est de savoir quelle quantité et quel genre de renseignements personnels les organismes canadiens fournissent aux organismes américains par le truchement de telles ententes sur l'échange de renseignements. À notre connaissance, personne ne connaît la réponse à cette question.

Nous croyons comprendre que le CIPVP a tenté, il y a quelques années, de vérifier ces ententes et n'a pu obtenir les renseignements fournis. Le CIPVP a de nouveau demandé la coopération des organismes au sein du gouvernement pour la collecte d'information relative aux ententes existantes sur l'échange de renseignements afin d'avoir une vue d'ensemble de la quantité des renseignements importants qui circulent. Nous croyons que votre comité comprendra l'impératif d'une vérification des protocoles et ententes en vigueur sur l'échange de renseignements et demandera au gouvernement d'assurer une pleine coopération avec le CIPVP dans ce travail urgent.

● (1550)

Meghan.

Mme Meghan McDermott (agente des politiques, Association des libertés civiles de la Colombie-Britannique): Je parlerai d'abord du précontrôle et des seuils concernant les fouilles.

Actuellement, les appareils électroniques sont considérés comme des biens dans le contexte de la frontière canadienne et dans les zones de précontrôle des aéroports canadiens, et il n'existe aucune mesure de protection prévue par la loi contre des fouilles arbitraires effectuées par des agents frontaliers. Les zones de précontrôle sont les zones désignées dans certains aéroports canadiens où les agents des États-Unis ont été habilités à traiter les voyageurs à destination des États-Unis.

Le projet de loi C-23, la Loi relative au précontrôle de personnes et de biens au Canada et aux États-Unis, a été présenté en juin dernier et vise à abroger et à remplacer la loi existante de 1999. Le projet de loi C-23 prévoit que les zones de précontrôle seront élargies au-delà des aéroports et pourraient être établies à des postes frontaliers ferroviaires, maritimes et terrestres. Il élargit les pouvoirs conférés aux agents américains, et, à notre avis, limite injustement les droits des voyageurs dans les zones de précontrôle. Nous avons exprimé nos préoccupations à l'égard de ce projet de loi lorsque nous avons comparu devant le Comité permanent de la sécurité publique et nationale et nous mettrons notre mémoire à la disposition du présent Comité également. En vertu de la loi relative au précontrôle existante et prévue, un voyageur ne peut faire l'objet d'une fouille à nu arbitraire. Un agent doit avoir un motif raisonnable de soupçonner afin d'avoir l'autorité légale de détenir le voyageur pour une fouille à nu.

Le CPVP a recommandé qu'un seuil identique pour la fouille d'appareils électroniques soit inscrit dans le projet de loi C-23. Dans une lettre adressée au Comité permanent de la sécurité publique et nationale, le CPVP demande « de modifier le projet de loi C-23 pour mettre la fouille d'appareils électroniques sur un pied d'égalité avec la fouille de personnes. De cette façon, un motif raisonnable de soupçonner un acte répréhensible serait obligatoire pour faire ce type de fouille. » L'ALCCB approuve cette position ainsi que la recommandation supplémentaire du CPVP visant une modification consécutive de la Loi sur les douanes afin de protéger de façon similaire la vie privée des Canadiens qui rentrent chez eux en franchissant les frontières canadiennes. Nous convenons avec le CPVP que « l'idée selon laquelle les appareils électroniques devraient être considérés comme de simples marchandiseset, par conséquent, pouvoir faire l'objet de fouilles sans motifs juridiques à la frontière est certainement dépassée et elle ne reflète pas les réalités de la technologie moderne ». Il est intéressant de noter que les documents de politique provisoires de l'ASFC semblent reconnaître qu'il est inapproprié de classifier des appareils numériques comme de « simples biens ». Un bulletin opérationnel de l'ASFC de 2015 ne prévoit pas de fouilles sans soupçon; il mentionne plutôt que des fouilles peuvent être menées s'il y a « des indications » que l'appareil numérique pourrait contenir la « preuve d'infractions ». Nous appuyons le CPVP qui demande que cette politique soit codifiée par des modifications législatives. La loi devrait obliger un agent frontalier, qu'il s'agisse de l'ASFC ou de l'agence américaine, dans une zone de précontrôle, à avoir des motifs raisonnables de soupçonner qu'une infraction à la loi a eu lieu avant qu'il puisse légalement fouiller un appareil électronique. Une telle loi fournirait une clarté et une transparence juridiques aux Canadiens tout en donnant à la politique actuelle force de loi. Elle appuierait également la reconnaissance, par la Cour suprême du Canada, du fait que la fouille d'appareils électroniques est une procédure extrêmement envahissante sur le plan de la vie privée.

Pour finir, j'aimerais aborder brièvement deux points. Le premier a trait au secret professionnel des avocats. L'Association du Barreau canadien a signalé cette question au Comité permanent de la sécurité publique et nationale, et elle s'applique aux passages frontaliers ordinaires ainsi qu'aux zones de précontrôle. Ni nous, ni l'ABC ne pouvons dire si le Canada a une politique définie au sujet des revendications de privilèges à l'égard de documents ou de dossiers électroniques sur nos appareils numériques. Ce privilège étant fondamental pour notre système juridique, nous voulons que le gouvernement élabore une politique reconnaissant le secret professionnel des avocats et qui permet aux voyageurs d'invoquer ce privilège à l'égard de renseignements physiques ou électroniques lorsqu'ils franchissent la frontière.

Deuxièmement, j'aimerais attirer votre attention sur notre recommandation visant à limiter les pouvoirs des agents américains de fouiller à nu des voyageurs au Canada en vertu du projet de loi C-23. Le mois dernier, au Comité permanent de la sécurité publique et nationale, nous nous sommes énergiquement opposés à ce que des pouvoirs soient conférés à des agents du précontrôle des États-Unis pour effectuer des fouilles à nu dans les zones de précontrôle au Canada. En vertu de la loi actuelle, un agent américain n'a pas l'autorisation légale de mener une fouille à nu à l'endroit de quiconque au Canada. S'il a des motifs raisonnables de soupçonner qu'une fouille à nu est nécessaire, l'agent canadien doit admettre que de tels motifs existent, et ce n'est qu'à ce moment qu'il peut mener cette fouille. Nous soutenons que seuls les agents canadiens devraient avoir le pouvoir d'effectuer les fouilles à nu au Canada, et dans des circonstances limitées, selon la loi.

● (1555)

Voilà qui conclut les propos que nous avons préparés. Nous serons heureuses de répondre à vos questions.

Le président: Merci beaucoup.

Chers collègues, la CPAC diffuse en direct sur mon téléphone. Le Président de la Chambre met la question aux voix maintenant, ce qui veut dire que la sonnerie retentira dans quelques secondes. Je demanderais le consentement unanime pour entendre les 10 prochaines minutes de témoignage. Ainsi, tous nos témoins auront la possibilité de comparaître avant que nous quittions la salle pour voter.

Consentez-vous unanimement à faire cela?

Des députés: D'accord.

Le président: Merci beaucoup.

Maître Bhandari, vous avez la parole pour 10 minutes.

Mme Esha Bhandari (avocate-conseil, Speech, Privacy, and Technology Project, American Civil Liberties Union): Merci beaucoup.

Je suis Esha Bhandari, avocate-conseil au service de l'American Civil Liberties Union. Nous apprécions l'occasion de comparaître devant le Comité aujourd'hui.

Je traiterai de deux sujets. Le premier est la protection des renseignements personnels à la frontière, et plus particulièrement la fouille des appareils électroniques. Le deuxième est le décret du président qui exclut les personnes qui ne sont pas des citoyens ou des résidents des États-Unis de la protection offerte par la Privacy Act.

En ce qui a trait à la fouille des appareils électroniques à la frontière, la position actuelle du gouvernement des États-Unis est qu'un régime de fouille sans soupçon est tolérable, selon la politique sur le Service des douanes et de la protection des frontières des États-Unis. Cette politique, qui date de 2009, autorise le gouvernement à fouiller tous les voyageurs, quel que soit le statut de citoyenneté, et à fouiller plus particulièrement leurs appareils électroniques sans mandat, cause probable ou soupçon de quelque nature que ce soit. La Cour suprême des États-Unis ne s'est pas encore prononcée sur cette autorité revendiquée. Quelques affaires de tribunaux inférieurs abordent la question, mais celle-ci demeure dans un domaine d'incertitude juridique, et plus précisément en ce qui concerne l'application éventuelle dans ce cas des limites constitutionnelles des États-Unis prévues par le quatrième amendement. L'ACLU est d'avis que les agents frontaliers ne devraient pas pouvoir fouiller des appareils électroniques sans cause probable au minimum, mais qu'un mandat est effectivement requis par la Constitution.

La nature des fouilles effectuées à la frontière peut varier. Il peut y avoir des fouilles manuelles ou sommaires, qui sont menées sur place lorsqu'un voyageur arrive à la frontière. Ces fouilles pourraient inclure la fouille des renseignements contenus sur l'appareil. Elles pourraient également inclure des fouilles des données infonuagiques qui sont accessibles au moyen de l'appareil, notamment par les médias sociaux et les applications de courriel. Nous sommes préoccupés par le fait que, lorsque les agents de la patrouille frontalière demandent à des personnes les mots de passe pour accéder à leurs appareils, ils ont accès à un nombre illimité de renseignements grâce aux applications infonuagiques connectées à Internet. Les citoyens américains ou les résidents permanents légitimes peuvent refuser de fournir les mots de passe permettant d'accéder à leurs appareils ou à leurs applications infonuagiques, mais les visiteurs risquent d'être refoulés s'ils refusent de le faire.

Un autre type de fouille est la fouille judiciaire. Lorsque cela se produit, le Service des douanes et de la protection des frontières (SDPF) des États-Unis saisira l'appareil, qu'il s'agisse d'un téléphone cellulaire ou d'un ordinateur portable, le transférera le plus souvent vers un autre lieu pour le brancher à un périphérique qui permet une fouille judiciaire complète de l'appareil. Il s'agit essentiellement d'une fouille à nu de l'ordinateur. Le gouvernement a accès non seulement à tout ce qui est en fait stocké sur l'appareil, mais également aux métadonnées et aux fichiers supprimés dont le voyageur n'est peut-être même pas conscient du fait qu'ils sont toujours accessibles au moyen de l'appareil.

Lorsque l'appareil est saisi de cette façon, le SDPF est censé le retenir pendant cinq jours seulement au départ, mais selon sa politique, cette période peut être prolongée par cycles de sept jours. Nous avons entendu des récits de personnes dont les appareils ont été saisis pendant des périodes pouvant aller jusqu'à des semaines. Selon la politique du gouvernement, tout renseignement pouvant être conservé doit avoir trait à l'immigration, aux douanes et à d'autres questions liées à l'application de la loi si le fait de les conserver est conforme aux normes en matière de protection de la vie privée et des données du système de dossiers dans lequel ces renseignements sont conservés. Cependant, nous sommes très préoccupés par des renseignements, comme ceux appartenant aux journalistes et à leurs sources ainsi que les renseignements relevant du secret professionnel des avocats, que la politique ne protège pas adéquatement. Les gens peuvent affirmer que ce type de renseignements est contenu sur leurs appareils avant qu'ils soient fouillés, mais en dehors de l'obligation de consulter un superviseur, il n'y a pas de limite pour le gouvernement américain en ce qui concerne les fouilles, même celles concernant ces renseignements privilégiés.

Bien que nous ayons entendu parler d'une augmentation non confirmée du nombre de fouilles, nous sommes également au courant d'une augmentation statistiquement documentée. Au cours de l'exercice 2015, le gouvernement des États-Unis déclare avoir mené 8 503 fouilles d'appareils électroniques à la frontière. Durant l'exercice 2016, ce nombre a bondi à 19 033. Bien que ces chiffres représentent un petit pourcentage de l'ensemble des voyageurs aux États-Unis, la forte hausse entre 2015 et 2016 est préoccupante, de même que l'absence de toute protection constitutionnelle du « soupçon » imposée à l'égard de ces fouilles.

● (1600)

Le besoin d'une plus grande transparence persiste. Nous ne savons à combien s'élève le nombre de fouilles menées en ce qui concerne des citoyens des États-Unis ou des non-citoyens et, dans le dernier cas, quels sont les pays dont les ressortissants font l'objet d'une fouille et pour quelle raison.

Je vais maintenant parler du décret du président, lequel exclut les personnes qui ne sont pas des citoyens ou des résidents des États-Unis de la protection offerte par la Privacy Act. Essentiellement, ce décret signifie que toute personne qui n'est pas américaine, c'est-à-dire quiconque n'est pas un citoyen ou un résident permanent légitime des États-Unis, n'a plus droit à la protection offerte par la Privacy Act. Ces mesures de protection incluent la capacité pour les personnes d'accéder à leurs dossiers, de les modifier et de limiter la diffusion et la collecte de renseignements par des organismes, sous réserve des exceptions mentionnées précédemment, dont le recours à l'application de la loi.

En raison d'une pratique de longue date, de nombreux organismes américains ont étendu la protection offerte par la Privacy Act afin d'inclure les renseignements personnels permettant d'identifier des personnes qui ne sont pas des citoyens ou des résidents des États-Unis, notamment les nombreux visiteurs ainsi que les étudiants et les gens d'affaires qui se rendent aux États-Unis à partir du Canada. Ces organismes comprenaient le département d'État, le département de la Sécurité intérieure, le département de la Justice et le département de la Santé et des Services sociaux. Plus particulièrement, en 2007, lorsque le département de la Sécurité intérieure a adopté la politique visant à étendre la protection offerte par la Privacy Act à toutes les personnes, il a souligné que cela aurait l'avantage de préserver l'intégrité des données, de promouvoir l'échange transfrontalier de renseignements, de faciliter le commerce et les déplacements et d'encourager la protection de la vie privée des citoyens des États-Unis à l'étranger.

Lorsque le décret a été signé, l'ACLU a envoyé une lettre à tous les organismes fédéraux, en faisant valoir que la mise en oeuvre du protocole tel que rédigé serait contraire à la loi, notamment qu'il supposait des obstacles procéduraux et juridiques importants. Nous avons également écrit au Parlement européen et à la Commission européenne pour leur faire savoir que les assurances des États-Unis qui sous-tendent l'accord de protection et l'accord-cadre É.-U.-UE pour permettre l'échange de données entre les deux régions seraient remises en question par ce décret.

Cependant, au moins le département de la Sécurité intérieure a publié des directives, en avril, indiquant son intention d'aller de l'avant avec les conditions du décret. Ces directives du département de la Sécurité intérieure précisent que les personnes qui ne sont pas des citoyens ou des résidents des États-Unis, y compris les immigrants et les non-immigrants, ne peuvent demander leurs dossiers que par l'entremise de la Freedom of Information Act plutôt que de la Privacy Act, et un critère de pondération s'appliquera désormais pour évaluer l'intérêt public à l'égard des renseignements au moment de décider de divulguer ou non les renseignements personnels de ces personnes. Cela comprend la divulgation possible à des tiers qui demandent des renseignements au sujet d'immigrants et de visiteurs aux États-Unis.

Les visiteurs et les immigrants aux États-Unis qui ne sont pas des citoyens ou des résidents de ce pays ne peuvent plus modifier leurs dossiers en vertu de la Privacy Act. Au lieu de cela, le département de la Sécurité intérieure a déclaré qu'il appliquerait désormais les principes de pratique équitable de traitement de l'information aux renseignements de ces personnes. Sur le plan pratique, on ne sait pas avec certitude ce que cela signifie. Il demeure très préoccupant de constater que les renseignements personnels des personnes qui ne sont pas des citoyens ou des résidents des États-Unis, des renseignements sensibles sur le statut d'immigration et des renseignements sur l'état de santé peuvent maintenant être divulgués publiquement puisque la protection offerte par la Privacy Act n'existe plus.

Je terminerai mon témoignage ici; je répondrai avec plaisir à vos questions.

Merci.

Le président: Merci beaucoup, maître Bhandari.

Chers collègues, comme la sonnerie se fera entendre dans un peu plus de 20 minutes, je vous recommande de suspendre la séance et d'aller faire notre devoir à la Chambre en allant voter.

J'ai tenté d'obtenir le consentement afin que nous puissions nous pairer, mais je ne pense pas que cela fonctionnera. Cela n'a jamais fonctionné auparavant, mais j'ai pensé que j'essaierais tout de même.

Si les témoins veulent bien patienter, nous suspendrons la séance tandis que les députés iront voter.

Mesdames et messieurs, si vous pouviez revenir ici dès que possible, nous devrions disposer de près de 40 minutes pour les questions. Nous commencerons par les interventions de sept minutes de sorte que nous pourrons tirer le maximum du temps qui nous reste par respect pour nos témoins.

Encore une fois, nous nous excusons auprès de nos témoins; nous n'avons pu avoir une réunion de comité plénier, mais c'est ce qui arrive à cette période de l'année. Je vous demanderais simplement d'être patients pendant que nous votons. Nous vous retrouvons dans 40 minutes environ.

● (1600)

(Pause)

● (1645)

Le président: Je vous remercie de votre patience, chers collègues et témoins, pendant que nous continuons à nous acquitter de nos responsabilités démocratiques ici.

Je vais maintenant passer à la série de sept minutes, et nous allons commencer par M. Long.

La parole est à vous, monsieur, pendant sept minutes. Faisons en sorte que nos questions et réponses soient le plus concises possible, car le Comité ne dispose plus que de 40 minutes.

M. Wayne Long (Saint John—Rothesay, Lib.): Merci du conseil, monsieur le président.

Merci à nos témoins. C'était un témoignage très intéressant et un agréable changement pour le Comité.

Il y a environ deux ans, j'ai traversé la frontière. Ma circonscription est Saint-John—Rothesay, dans le sud du Nouveau-Brunswick, et nous sommes près de la frontière du Maine, évidemment, qui est environ à une heure de distance. Nous avons franchi la frontière, et les douanes américaines nous ont bien sûr demandé de garer la voiture. On nous a dit d'aller dans le bâtiment et on nous a demandé de laisser nos téléphones cellulaires dans la voiture.

Nous sommes entrés dans le bâtiment et nous avons été interrogés pendant probablement 10 ou 15 minutes. Mon fils participait à des courses de moto tout terrain, alors nous étions souvent à la frontière. Nous avons probablement attendu de 20 à 25 minutes. On nous a dit que nous pouvions partir, et nous sommes retournés à notre voiture. Il n'y avait pas de téléphones dans la voiture.

Nous sommes revenus à l'intérieur, et on nous a remis les téléphones, mais il y a eu peut-être une période de 30 à 40 minutes pendant laquelle nous n'avions pas les téléphones. Les agents sont sortis avec les téléphones, et ils ont demandé à mon fils de déverrouiller son téléphone. Il l'a fait, et encore une fois, ils ont disparu. Bref, nous avons récupéré les téléphones, mais c'était certainement inquiétant et troublant pour nous tous.

Dans quelle mesure chacun d'entre vous est-il préoccupé par des dispositifs de clonage et de copie en miroir, car j'entends que les organismes ont de plus en plus recours à ces dispositifs? De toute évidence, ils pouvaient suivre ce qui se passait bien après que nous avons quitté cette frontière. À votre avis, cela devient-il plus pertinent à mesure que nous avançons dans cette ère de sécurité accrue?

Maître Bhandari.

Mme Esha Bhandari: Merci beaucoup de votre question, monsieur Long.

En fait, je suis originaire de Saint John et je suis une fière diplômée de l'école secondaire Saint John. C'est agréable de vous parler.

Nous essayons de suivre la piste de la technologie acquise par le Service des douanes et de la protection des frontières des États-Unis. L'un des principaux domaines sur lesquels nous nous sommes concentrés est l'utilisation de dispositifs comme Cellebrite, qui permet d'effectuer des fouilles judiciaires.

Dans le cadre de demandes faites en vertu de la Freedom of information Act et de diverses initiatives de journalisme d'enquête, on s'est efforcé de suivre les sommes dépensées pour une technologie en particulier. Bien qu'il s'agisse d'une préoccupation, je pense que nous n'en savons pas encore assez sur la nature de ces capacités à la frontière précisément — et dans votre cas en particulier, celles qui se trouvaient vraisemblablement à une frontière terrestre pendant une courte période lorsque vos téléphones étaient hors de vue — par rapport aux capacités, si les téléphones sont saisis et apportés dans une installation offrant un plus grand accès à la technologie.

Nous sommes très préoccupés par toute technologie acquise dans ce domaine et utilisée à la frontière, mais je ne crois pas que nous disposons de suffisamment d'information maintenant.

● (1650)

M. Wayne Long: D'accord.

Et qu'en est-il en Colombie-Britannique?

Mme Micheal Vonn: La seule chose que je mentionnerais, c'est que nous avons souvent affirmé que nous avons besoin d'accroître la transparence en ce qui concerne tous ces appareils de surveillance qui existent. En outre, il faudrait que le CPVP ait accès à des évaluations des facteurs relatifs à la vie privée pour l'ensemble de ces appareils, peu importe la façon dont ils sont utilisés — ou qu'ils soient utilisés ou non — à la frontière canadienne. Nous savons qu'au Canada, cela ne se fait pas pour les appareils de surveillance de masse.

Malgré tout, nous déployons aussi des efforts, comme l'ACLU, pour suivre la piste de ces appareils.

M. Wayne Long: Madame McPhail, voulez-vous ajouter quelque chose?

Mme Brenda McPhail: À nouveau, je dirais que cela nous préoccupe aussi.

La transparence et la reddition de comptes aux postes frontaliers passent, en partie, par notre capacité de comprendre — comme je l'ai dit dans mon exposé — ce qui se passe lorsque nos appareils qui contiennent des renseignements sont saisis.

J'aimerais souligner le fait que nous ne sommes pas seulement préoccupés par les technologies qui sont utilisées et le fait qu'il soit possible de copier de l'information à partir d'un téléphone. Nous sommes aussi très inquiets, car nous ne savons pas dans quelle mesure ces renseignements sont communiqués à d'autres entités.

M. Wayne Long: D'accord.

Puisque Me Bhandari vient de Saint John, je vais m'adresser de nouveau à elle.

Vos chiffres sont légèrement différents des miens. D'après un rapport que j'ai lu, entre octobre 2015 et septembre 2016, il y a eu « cinq fois plus de fouilles d'appareils électroniques — soit 23 877 — menées par des agents aux États-Unis ». Je crois que vous avez dit que c'était environ 19 000. Dans le rapport, il est indiqué que « selon NBC, 5 000 fouilles ont été effectuées en février seulement ».

Comment pouvons-nous mettre un frein à cette tendance? Clairement, cela va en s'augmentant, et ça ne va pas arrêter. Le risque est-il si grand que nous devons donner aux agents tout ce qu'ils demandent, essentiellement, lorsque nous voulons aller aux États-Unis? C'est assez évident qu'ils peuvent empêcher quelqu'un d'y entrer pour presque n'importe quel motif maintenant, n'est-ce pas?

Mme Esha Bhandari: Les statistiques que vous avez vues ont d'abord été divulguées par le gouvernement américain, mais depuis, elles ont été revues à la baisse, ce qui explique cette différence de 23 000 à 19 000. Malgré tout, même avec cette correction à la baisse, il est clair qu'il y a eu une hausse soudaine.

Nous déployons des efforts sur un certain nombre de fronts afin que la situation change, entre autres, bien sûr, la voie juridique. On attend toujours les décisions des tribunaux américains de diverses instances. La plupart du temps, le sujet est abordé dans un contexte de poursuites au criminel lorsque quelqu'un conteste la fouille de son téléphone à un poste frontalier. C'est possible que la voie juridique rehausse la norme en vigueur en ce qui concerne les fouilles. Il faut qu'il y ait un certain niveau de soupçons.

Notamment, un tribunal de la United States Court of Appeals for the Ninth Circuit a rendu une décision — c'était l'un des tribunaux du circuit Ouest — selon laquelle il faut qu'il y ait un doute raisonnable pour procéder à une analyse criminalistique, en particulier si la fouille doit avoir lieu à l'extérieur du site ou s'il s'agit d'une fouille invasive. Nous avons cherché à obtenir des dossiers montrant que la décision est respectée, mais jusqu'à présent, rien ne nous permet de conclure que des politiques ont été modifiées afin de refléter la nouvelle exigence, soit qu'il faut qu'il y ait un certain niveau de soupçons. Malgré tout, les affaires judiciaires se poursuivent, et c'est une priorité.

Ensuite, il y a la voie législative. Selon une loi nationale qui a été proposée, il serait obligatoire d'obtenir un mandat pour fouiller des appareils. Cependant, cela ne s'applique qu'aux citoyens américains et aux résidents permanents légitimes. Donc, cela ne protégerait pas les Canadiens à la frontière. On ne s'en est pas soucié dans ce projet de loi.

Pour finir, nous réclamons également une plus grande transparence. Selon nous, ce n'est pas suffisant de publier des chiffres. Essentiellement, nous croyons que nous devons être au courant de la nationalité des personnes fouillées ainsi que les motifs pour lesquels elles l'ont été. C'est difficile de définir avec certitude pourquoi on veut le téléphone de certaines personnes, mais pas d'autres, surtout puisque, conformément à la politique en vigueur, les agents peuvent procéder à des fouilles en l'absence de tout soupçon.

● (1655)

Le président: Merci beaucoup.

La parole va maintenant à M. Jeneroux, pour sept minutes. Allez-y.

M. Matt Jeneroux (Edmonton Riverbend, PCC): Merci, monsieur le président

Merci beaucoup à tout le monde d'être venu aujourd'hui, de s'être préparé à la séance et de nous avoir attendus pendant que nous votions. Ces votes ne sont pas une partie de plaisir.

Ma question s'adresse à tout le monde. J'ai consulté un peu de documentation sur le sujet, et j'ai remarqué que les attentes sont inférieures par rapport à la protection de la vie privée aux postes frontaliers dans les aéroports ou aux postes frontaliers terrestres. Si j'ai dit cela, c'est à cause de deux documents précis: le propre document du commissaire à la protection de la vie privée, intitulé « Votre droit à la vie privée dans les aéroports et aux postes frontaliers », ainsi que l'arrêt R. c. Simmons de la Cour suprême, qui remonte à 1988. Dans cet arrêt, le tribunal mentionne que « les voyageurs qui cherchent à traverser les frontières internationales s'attendent parfaitement à faire l'objet d'un processus d'examen ». Ce n'est qu'après l'avoir lu que j'ai commencé à y réfléchir. Il semble vraiment que les attentes soient plus basses, parce que nous devons passer les contrôles de sécurité, et de nos jours, par les scanners.

Peut-être pourriez-vous nous dire si, selon vous, cela est dû à une loi en vigueur ou s'il s'agit simplement d'une norme de société qui a évolué depuis la création des aéroports.

Peut-être pourrait-on commencer avec vous, maître Bhandari.

Mme Esha Bhandari: Bien sûr. Merci beaucoup.

Selon moi, quelques-uns des facteurs qui sous-tendent votre supposition ne tiennent plus lorsqu'il s'agit de la fouille d'appareils électroniques. D'abord, on tient pour acquis que les voyageurs peuvent décider de ce qu'ils apportent avec eux pour franchir la frontière, et c'est pourquoi les lois, les politiques et le droit jurisprudentiel, dans le passé, posait en postulat que les voyageurs, qui sont parfaitement conscients de ce qu'ils transportent avec eux de l'autre côté de la frontière, savent que les agents aux postes frontaliers doivent les fouiller pour vérifier s'ils ont des articles de contrebande ou des choses qui ne doivent pas franchir la frontière.

Lorsqu'il s'agit d'appareils électroniques, on ne peut pas tenir ce genre de choses pour acquis, puisque ces appareils contiennent une montagne de renseignements. Si on part du principe que le téléphone d'une personne est connecté à Internet, est donc connecté à son courriel, à ses comptes de médias sociaux et à tous ses autres comptes ainsi qu'à ses renseignements financiers, d'une certaine façon, le voyageur transporte avec lui ce genre de renseignements et s'expose très concrètement au risque d'être fouillé. Je ne crois pas que la même justification peut s'appliquer ici, et c'est pourquoi je crois que nous devons vraiment contester cette notion qui veut que les motifs de fouille aux douanes s'appliquent aux appareils électroniques.

Je crois que cela est particulièrement clair lorsqu'il s'agit des fouilles à des fins d'enquête criminelle. Comme je l'ai déjà mentionné, il est possible de retrouver des éléments qu'une personne a effacés pour les fouiller. Le gouvernement peut y avoir accès. Encore une fois, les gens ne peuvent pas véritablement décider de ce qu'ils transportent avec eux lorsqu'ils traversent la frontière, et c'est pourquoi je ne crois pas qu'on puisse dire que les gens ont des attentes moins élevées en ce qui concerne la protection de leur vie privée dans le monde numérique.

M. Matt Jeneroux: Maître Vonn et maître McDermott.

Mme Micheal Vonn: Oui, je suis tout à fait d'accord avec tout ce que vous avez dit.

Je voudrais simplement ajouter que des attentes moins grandes par rapport à la protection de la vie privée ne veulent pas dire qu'il n'y a aucune attente de protection de la vie privée. Le respect de la Constitution à la frontière est sans cesse remise en question et redéfinie non seulement par l'arrivée de nouveaux médias et de nouveaux appareils électroniques, mais également par d'autres choses, par exemple ce qui a été mentionné par notre collègue de l'ACLC. Je parle des mots de passe, de l'obligation de les fournir ainsi que tout le reste, et si cela correspond ou non à une entrave à la justice. Toutes ces politiques comprennent tellement de zones grises en ce qui concerne la portée du cadre constitutionnel que nous évoluons certainement dans un vide informationnel.

M. Matt Jeneroux: Madame McPhail.

Mme Brenda McPhail: Je vais préserver l'harmonie et me ranger du côté des deux précédents intervenants.

Je crois qu'il est très important de définir la différence entre un téléphone, qui est pratiquement une fenêtre sur votre vie et une valise, remplie de bas, de sous-vêtements et peut-être d'une ou deux paires de jeans. Qualitativement, il s'agit de choses différentes, et nous les traitons de la même façon. Selon nous, cela n'a absolument aucun sens.

Même si notre position est que la sécurité de nos frontières est très importante et qu'elles doivent être fortes, ou que nous ne voulons pas laisser entrer de mauvais éléments — c'était d'ailleurs l'un des principes sous-tendant la Loi sur les douanes, le fait que nous ne voulons pas que de mauvais éléments traversent notre frontière —, les documents électroniques sur un appareil ne sont pas une « chose », dans n'importe quel sens du terme. Ce n'est pas une chose qu'on importe au Canada de façon concrète, puisqu'ils vont continuer d'exister qu'ils traversent ou non la frontière. Ces documents peuvent traverser la frontière avec un humain ou de façon virtuelle, en ligne. Le document n'entre d'aucune façon physique au pays, ce qui fait que le document ne pose aucun risque en particulier pour la sécurité nationale ou pour la souveraineté du Canada. Voilà les principes sur lesquels on devrait s'appuyer pour dire qu'on devrait étendre les pouvoirs relatifs à la fouille aux postes frontaliers, parce que ces deux choses, la sécurité nationale et la souveraineté, sont très importantes. Pour ces raisons, nous croyons qu'il est temps de mettre à jour la loi en prenant en considération les différences fondamentales qui existent entre un appareil électronique et une valise.

● (1700)

M. Matt Jeneroux: Je crois que je vais formuler quelques commentaires et espérer que vous pourrez donner votre opinion sur le sujet. Si on tient pour acquis que les gens vont hésiter à envoyer du matériel — disons qu'il s'agit de documents illégaux — par voie électronique... vous vous demandez si le serveur est sécurisé, et tout le reste, ce qui ne s'applique pas à un appareil électronique que vous remettez à quelqu'un en lui disant « tiens! », voici le document illégal.

Il semble que toute menace n'est pas écartée ici. Une personne pourrait tout de même transporter quelque chose dans son téléphone parce qu'elle n'est pas à l'aise de l'envoyer en utilisant un serveur.

Mme Brenda McPhail: Je crois qu'on devrait probablement examiner les questions relatives aux menaces en prenant en considération ce qui est fait pour les documents protégés par le secret professionnel de l'avocat. C'est un peu le même contexte pour cette question. Lorsqu'on juge que des documents sont privés parce qu'ils sont liés à une affaire, et lorsque ce privilège est reconnu dans n'importe quel autre contexte, il n'y a aucune raison pour laquelle le même privilège ne devrait pas s'appliquer ailleurs. Ces documents ne sont pas plus dangereux à la frontière que s'ils étaient ici dans cette salle.

M. Matt Jeneroux: D'accord.

Mon temps est écoulé, n'est-ce pas?

Le président: Je crois que oui.

Monsieur Dubé, vous avez sept minutes. Allez-y, je vous prie.

[*Français*]

M. Matthew Dubé (Beloeil—Chambly, NPD): Merci, monsieur le président.

Ma question s'adressera à la représentante de l'American Civil Liberties Union, ou ACLU, mais je commencerai par m'adresser aux deux associations canadiennes.

Je vous remercie tous d'être parmi nous. Tout comme mes collègues avant moi, je vous remercie d'avoir fait preuve de patience, compte tenu des votes et de tous les beaux moments que nous vivons à la fin d'une session parlementaire.

On parle souvent d'une directive ministérielle provenant du ministre de la Sécurité publique concernant la fouille des appareils électroniques. Cette directive ne constitue pas une loi, je le rappelle. Cette distinction est importante. Selon nous, la directive, contrairement à ce qu'on prétend, est beaucoup trop permissive et octroie beaucoup de pouvoir aux agences des services frontaliers.

Les représentants de l'Association canadienne des libertés civiles et de l'Association des libertés civiles de la Colombie-Britannique souhaitent-ils faire des commentaires à cet égard?

[*Traduction*]

Mme Brenda McPhail: Je suis profondément navrée, mais je n'ai pas l'appareil pour l'interprétation. Je ne comprends pas ce que vous dites.

Le président: Ah, Seigneur.

[*Français*]

M. Matthew Dubé: Nos amis de l'Association des libertés civiles de la Colombie-Britannique aimeraient-ils formuler des commentaires?

[*Traduction*]

Mme Micheal Vonn: Bien sûr.

Par directive, j'imagine que vous parlez des récents décrets présidentiels aux États-Unis et comment...

M. Matthew Dubé: Non, je parle du Canada, des directives ministérielles concernant le téléphone cellulaire. Le gouvernement nous dit de consulter ces directives dès que nous posons une question.

Mme Micheal Vonn: Donc, il s'agit d'une directive interne de l'ASFC?

M. Matthew Dubé: C'est exact.

Mme Micheal Vonn: D'accord, merci.

Notre position à ce sujet comprend deux volets: premièrement, on semble reconnaître dans cette directive qu'une fouille en l'absence de tout soupçon n'est pas appropriée en ce qui concerne les appareils électroniques. Cependant, comme vous l'avez dit, cette directive n'est pas reflétée dans une loi, quelle qu'elle soit. Il ne s'agit que d'une orientation.

Le CPVP et nous aimerions qu'on donne du mordant à cette directive, c'est-à-dire adopter un amendement en conséquence dans la Loi sur les douanes afin que la directive puisse et doive être appliquée. Cela en ferait une pratique concrète — s'il s'agit vraiment d'une pratique, puisque nous n'avons aucun moyen de le vérifier dans la présente situation — qui serait reflétée dans la loi. Nous pourrions ainsi nous prévaloir de la loi et dire: « voilà la façon dont les choses doivent être faites. »

● (1705)

[*Français*]

M. Matthew Dubé: Parlons d'un exemple précis lié au projet de loi C-23 et au fait que cela n'est pas prescrit dans la loi.

Si nous nous fondons sur les protections accordées par la loi canadienne, il est possible de conclure que, s'il y avait un décret présidentiel du côté américain et si la loi canadienne était muette là-dessus, la protection des voyageurs dont on voudrait fouiller le téléphone cellulaire, par exemple, ne serait pas assurée. Est-ce exact?

[*Traduction*]

Mme Micheal Vonn: Oui, c'est notre interprétation, indéniablement.

[*Français*]

M. Matthew Dubé: Madame McPhail, je peux vous poser de nouveau la question sur la directive relative à l'Agence. Avez-vous des commentaires à faire à cet égard?

[*Traduction*]

Mme Brenda McPhail: Je crois que cela illustre parfaitement le fait qu'on ne peut pas s'attendre à ce que les lois demeurent statiques. Vous ne pouvez pas dire que ce n'est pas grave si on adopte une mauvaise loi, parce que la personne au pouvoir ne va jamais rien faire de mal en l'appliquant. Nous devons être prudents et nous assurer que ce que nous avons est bien interprété et nous protège de la façon escomptée.

Aux États-Unis, où les lois sont essentiellement créées par décrets présidentiels, on voit bien, à titre d'exemple, la façon dont la primauté du droit peut être attaquée lorsqu'il n'y a pas, d'emblée, des lois solides, efficaces et claires en vigueur, qui sont plus difficiles à contester.

[*Français*]

M. Matthew Dubé: Merci.

[*Traduction*]

Je m'adresse à Me Bhandari: du point de vue des Américains, en quoi les risques de profilage sont-ils accrus par les renseignements qu'on peut trouver dans le téléphone cellulaire d'une personne? Je vais simplement donner un exemple précis pour mettre la question dans son contexte.

Il s'agit du cas survenu il y a quelques mois; un homme de Vancouver se rendait dans l'État de Washington, et l'accès lui a été refusé à la frontière parce que, quand les douaniers ont découvert son orientation sexuelle, par le truchement de son téléphone cellulaire, ils ont présumé à tort que cette personne se rendait aux États-Unis dans le but d'y exercer la prostitution, ce qui était manifestement une situation de profilage flagrante.

De ce point de vue, y a-t-il également lieu d'être préoccupé, non seulement en raison du caractère intrusif de fouiller dans les téléphones cellulaires, mais aussi puisqu'on crée essentiellement une longue liste de stéréotypes et de préjugés qui peuvent être utilisés contre un voyageur d'une manière inappropriée comme celle-là?

Mme Esha Bhandari: Nous sommes très préoccupés à ce sujet. Nous avons formulé des commentaires publics dans le contexte des nouvelles procédures de contrôle censément extrêmes qui ont été appliquées à certains demandeurs de visa. Le gouvernement américain a maintenant commencé à chercher dans les médias sociaux des renseignements sur des demandeurs provenant de certains pays. Je pense que les mêmes préoccupations se posent lorsqu'il est question de renseignements recueillis dans un téléphone cellulaire, ce qui — comme je l'ai mentionné — pourrait comprendre les médias sociaux. Sans politiques expliquant les lignes directrices relatives à l'utilisation de ces renseignements, sans règles limitant le pouvoir discrétionnaire de chaque douanier, et si l'on ne précise pas réellement l'utilisation qui doit être faite de ces renseignements, la voie est essentiellement ouverte pour que chaque agent des visas ou des services frontaliers puisse soumettre les gens à du profilage, prendre les renseignements hors contexte et refuser l'accès aux gens ou les priver de droits sans même leur donner la possibilité de répondre. Nous pensons que la fouille des appareils électroniques fait augmenter grandement ce risque que des renseignements soient recueillis sans contexte et sans aucune explication de la façon dont ils peuvent être utilisés pour déterminer l'admissibilité.

M. Matthew Dubé: On entend toujours parler de ces décrets, et vous avez mentionné un projet de loi qui est soumis à l'étude du Congrès, si je ne m'abuse. De votre point de vue, dans quelle direction avez-vous l'impression que cela va aller?

Mme Esha Bhandari: C'est difficile à prévoir. Les tribunaux pourraient trancher à l'égard de certaines de ces questions. Les décisions des tribunaux pourraient porter sur le genre d'exigences de base relatives aux fouilles. Selon moi, il va falloir que l'on défende les droits des gens pour que les politiques changent lorsqu'il est question de recueillir des renseignements dans les médias sociaux. Je pense que ce principe s'applique même aux renseignements qui sont accessibles au public. Nous sommes très préoccupés au sujet des conséquences sur la liberté d'expression et sur les droits de la personne dans le monde entier, si le fait que les gens doivent révéler le justificatif d'identification de leurs médias sociaux devient une condition pour voyager. Cette condition peut avoir une énorme incidence sur les personnes qui ont un compte anonyme, par exemple — de nombreux militants ont des comptes anonymes —, et sur de nombreuses personnes qui n'ont peut-être pas envie que tout le monde connaisse leur identité. Alors, je pense que ce genre de collecte de renseignements dans de multiples contextes suscite de vastes préoccupations relativement à la liberté d'expression, à nos yeux.

● (1710)

Le président: Merci beaucoup, monsieur Dubé.

Nous passons maintenant à notre dernière question de sept minutes, de M. Saini. Ensuite, je pense qu'il nous restera du temps pour deux ou trois périodes de questions de cinq minutes, puis seulement quelques minutes, à la fin, pour certains travaux du Comité.

Monsieur Saini, allez-y, s'il vous plaît.

M. Raj Saini (Kitchener-Centre, Lib.): Bonjour, tout le monde.

Maître Bhandari, ma première question s'adresse à vous, puisque vous êtes aux États-Unis.

J'ai beaucoup de difficulté à comprendre cela, car vous parliez de quelque chose qui se passe aux États-Unis, actuellement, comme le fait qu'il y a un très fort sentiment de sécurité nationale. D'une part, vous avez un décret, qui ne va pas protéger les renseignements personnels des personnes qui ne sont pas des citoyens américains. Vous avez un bouclier de confidentialité majeur entre l'Union européenne — qui comprend 28 pays — et les États-Unis; et vous avez une entente semblable avec le Canada et probablement avec d'autres pays du monde. N'est-il pas un peu ironique que les États-Unis exigent que la vie privée des citoyens américains soit équivalente à celle des citoyens d'autres pays ou aussi importante pour s'assurer qu'il y a une réciprocité avec le reste du monde? Quel est le sentiment à cet égard? Je ne comprends pas. Pouvez-vous formuler des commentaires concernant la raison pour laquelle les Américains font cela? À mes yeux, on dirait qu'ils réduisent leur sécurité nationale, car ils exposent leurs propres citoyens à des risques, puisque, dans certains cas, d'autres pays pourraient ne pas être aussi prudents en ce qui a trait à la protection de leurs droits à la vie privée. Pourriez-vous seulement souligner en quelque sorte les raisons pour lesquelles cette situation se produit?

Mme Esha Bhandari: En ce qui concerne la Privacy Act, je pense que le décret a été adopté, bien franchement et malheureusement, dans le but de permettre la création de ce bureau pour les victimes d'actes criminels commis par des immigrants. Un malheureux discours circule au sujet de la diffusion publique des crimes commis par des immigrants et, par conséquent, du besoin de retirer des mesures de protection de la Privacy Act dans le but de communiquer cette information au public. Nous avons déjà observé un effet malheureux de cette situation, c'est-à-dire qu'une base de données récemment publiée supposément dans le but de fournir des renseignements au sujet d'immigrants qui auraient commis des actes criminels contenait des renseignements au sujet de victimes de violence conjugale et de mauvais traitements, des personnes dont les renseignements devraient être protégés. La communication de ces renseignements au public les place certainement à risque. Je pense que le but de la création de ce bureau est lié au décret de la Privacy Act.

Il est certain que, dans la lettre que nous avons adressée au Parlement européen et à la Commission européenne, nous avons souligné comment cela mine cette entente et, encore une fois, dans le cadre des activités de défense des droits que nous menons aux États-Unis, nous signalons également que la préoccupation relative à la réciprocité est réelle. Les Américains qui voyagent vers d'autres pays pourraient se voir demander de fournir des renseignements semblables — leurs mots de passe de médias sociaux, leurs adresses de courriel et l'accès à leur téléphone —, ce qui devrait susciter d'énormes préoccupations pour le gouvernement américain également.

M. Raj Saini: Ma deuxième question s'adresse à tous.

Je suis certain que vous êtes conscients du fait que le Congrès américain a récemment annulé des dispositions réglementaires instaurées par l'administration Obama pour la réglementation des FSI. Le marché de la publicité en ligne vaut 83 milliards de dollars, et, maintenant, il y a une récusation des FSI concernant l'obligation de respecter les mêmes protocoles en ce qui a trait à l'historique de navigation d'une personne, à son utilisation d'applications et à l'endroit où elle se trouve. Tout cela est maintenant exposé et conservé aux États-Unis, alors, dans le cas des personnes qui font continuellement des voyages aller-retour, y a-t-il lieu d'être préoccupé au sujet de l'exposition?

Je parle plus précisément des Canadiens et d'autres personnes qui visitent les États-Unis.

N'importe qui peut commencer.

Madame McPhail.

Mme Brenda McPhail: Je pense que, lorsque nous entendons parler de ce retrait régressif de mesures de protection des renseignements personnels qui avaient été durement acquises, bien sûr que c'est préoccupant.

Je n'arrive pas à déterminer clairement à quel degré de risque les Canadiens font face, mais, la réalité, c'est que notre vie en ligne n'est pas limitée par des frontières. Nous faisons affaire avec des entreprises américaines, et nous naviguons sur des sites appartenant à des entreprises américaines. Je n'en suis pas certaine, mais je suppose que nous devrions être préoccupés, car nos renseignements vont inévitablement se retrouver pris exactement dans le même filet que ceux des Américains, du fait qu'il n'y a aucune réglementation au sujet de la non-communication de ce genre de renseignements.

S'il y a un certain degré de protection au Canada, évidemment, lorsqu'il est question d'une loi mentionnant les FSI, c'est que la plupart d'entre nous sont probablement abonnés auprès d'un fournisseur de services canadien ici, au Canada, mais un grand nombre de ces entreprises de télécommunication ont une portée mondiale et sont reliées par un même réseau de diverses manières; nous en connaissons certaines, en tant que citoyens ordinaires, mais il y en a bien d'autres que nous ne connaissons pas. Cependant, encore une fois, ces genres de liens pourraient mettre les renseignements à risque.

● (1715)

M. Raj Saini: Maître Vonn.

Mme Micheal Vonn: Je n'ai rien d'important à ajouter à cela.

M. Raj Saini: Y a-t-il quelqu'un d'autre?

Maître Bhandari, je regrette de m'acharner sur vous, mais, comme vous êtes aux États-Unis, connaissez-vous, en ce qui concerne la protection des renseignements personnels...? Si vous regardez ce qui arrive à la FTC, surtout sa conception de la neutralité d'Internet, cela peut aller dans un sens comme dans l'autre. Voyez-vous ou prévoyez-vous quoi que ce soit? Pensez-vous que la situation va empirer ou s'améliorer, ou bien y a-t-il un genre de tollé de protestations aux États-Unis ou un genre de recul visant à corriger ce décret, ou, du moins, à tenter d'atténuer la friction entre la FTC et la FCC, surtout au sujet de la neutralité d'Internet?

Mme Esha Bhandari: Oui, je pense qu'il va y avoir un énorme recul et qu'il y en a déjà un. La première bataille pour la neutralité d'Internet s'est déroulée ici. Je pense que les gens attendent le deuxième round.

C'est un énorme enjeu. Le même milieu et la même coalition que ceux qui ont lutté pour la neutralité d'Internet la première fois sont encore mobilisés. Je dirais la même chose de la question des FSI.

De fait, je pense que le Congrès a peut-être été surpris par la mesure dans laquelle cet enjeu a beaucoup été abordé, a suscité beaucoup d'attention et a fait l'objet de beaucoup d'opposition, plus que prévu.

M. Raj Saini: Merci beaucoup

Le président: Merci, monsieur Saini.

Nous allons maintenant passer à M. Kelly; vous avez la parole, pour une période de cinq minutes.

M. Pat Kelly (Calgary Rocky Ridge, PCC): Merci.

Je voudrais avoir une idée de certains des problèmes qui ont été recensés en fonction d'anecdotes. Je ne veux pas critique cette méthode de recensement des problèmes. En tant que représentants élus, nous le faisons tout le temps. Les électeurs viennent nous raconter leurs problèmes, et nous savons que de nombreux Canadiens veulent un processus prévisible, harmonieux et efficient à la frontière. Ils veulent également être protégés contre les menaces externes, alors il y a beaucoup d'enjeux complexes qui vont de pair avec la sécurité frontalière.

J'ai été frappé par quelques-unes des données que nous avons obtenues concernant les appareils fouillés à la frontière. Si je l'ai bien pris les chiffres en note, il y en a eu un peu plus de 8 500 en 2015 et 19 000 en 2016, soit le double. On pourrait dire qu'il s'agit d'une tendance, le double en un an. Je ne sais pas quel pourrait être le nombre en 2017.

Que sait-on au sujet de ces fouilles d'appareils? Avons-nous la moindre idée de l'identité des propriétaires des appareils, par nationalité, qui ont été fouillés à la frontière américaine?

Mme Esha Bhandari: Nous ne savons pas grand-chose de plus que ces nombres. Il y a actuellement une poursuite en instance visant à obtenir plus de renseignements, à obtenir précisément les documents que vous avez mentionnés: la nationalité des personnes fouillées et les motifs.

M. Pat Kelly: D'accord, alors nous ne savons pas si ce sont surtout des Canadiens, par exemple. Nous n'avons vraiment aucune idée.

Mme Esha Bhandari: Non. L'ACLU a obtenu certains documents, vers la période de 2008 à 2010, et je dirais qu'environ la moitié des fouilles menées durant cette période visaient des citoyens américains, mais nous ne savons pas pour l'autre moitié.

M. Pat Kelly: D'accord. Savons-nous même quels types de renseignements sont recherchés durant la fouille d'un appareil? Avons-nous même des renseignements anecdotiques? M. Dubé a mentionné le cas particulier d'un résident de Vancouver. Que cherche-t-on en procédant à ces fouilles d'appareils, quelles sont certaines des autres plaintes formulées par les personnes dont l'appareil a été fouillé, et quels ont été les résultats de ces fouilles?

Mme Esha Bhandari: Nous ne le savons pas systématiquement. Les personnes qui sont des citoyens américains et qui ont été lésées par la fouille d'un appareil pourraient parfois présenter une plainte administrative visant à accéder aux dossiers de leur téléphone qui ont été conservés. Cet accès pourrait donner aux personnes une indication de ce qui a été tiré de leur téléphone, des dossiers ou des notes qui ont été conservés par le gouvernement. Toutefois, nous n'avons pas établi de politique systématique déclarant ce qui a été fouillé, quelles sont les conditions de la fouille et ce qui a été conservé. Nous savons que le gouvernement est censé détruire les copies des renseignements tirés d'une fouille s'il ne trouve aucune cause probable de la perpétration d'une infraction. Encore une fois, nous ne savons pas à quelle fréquence les douaniers trouvent une cause probable, à quelle fréquence ils détruisent les renseignements comme ils sont censés le faire, selon la politique. Ce sont tous des renseignements qui n'ont pas été révélés.

● (1720)

M. Pat Kelly: D'accord. Je comprends le point qu'a soulevé Mme McPhail, un téléphone n'est pas un objet de contrebande en soi par exemple... de la même façon que les gens ont longtemps été habitués à être fouillés à la frontière. Quel type de justification et quels types de renseignements possèdent les agents d'application de la loi ou encore, quelles plaintes ont été formulées par des Canadiens à propos d'articles qui ont été fouillés ou quels comportements sont possiblement recherchés par les autorités frontalières?

Mme Brenda McPhail: Nous n'en savons pas beaucoup en ce qui concerne le contexte canadien. L'ASFC n'a pas fourni les chiffres que l'ACLU peut nous fournir au sujet des fouilles d'appareils électroniques aux États-Unis. Nous ne connaissons même pas le nombre approximatif d'appareils fouillés, peu importe ce qu'on cherchait. Nous ne savons pas nécessairement ce que cherchent les autorités. Nous ne savons pas ce qui est confisqué. Nous ne savons pas combien de temps ces articles peuvent être conservés. Il y a vraiment un grand manque d'information.

Si on revient aux données empiriques et qu'on s'éloigne de la collecte systématique de données, on entend parler de téléphones qui ont fait l'objet d'une fouille, semble-t-il, parce qu'on cherchait des reçus pour des marchandises ayant été achetées de l'autre côté de la frontière, ce qui est tout à fait logique, sauf qu'après, ils ferment le courriel et se mettent à parcourir les photos juste pour voir s'ils ne trouveraient pas quelque chose d'osé.

M. Pat Kelly: Très rapidement, parce qu'il ne me reste plus de temps, quelqu'un sait-il quel est le nombre total de personnes qui sont allées aux États-Unis par rapport aux 20 000 personnes fouillées?

M. Raj Saini: Trois cent quatre-vingt-dix millions.

M. Pat Kelly: D'accord, merci.

Une voix: Des centaines de millions.

M. Pat Kelly: D'accord.

Le président: Merci, monsieur Kelly.

Monsieur Erskine-Smith, ramenez-nous à la maison s'il vous plaît.

M. Nathaniel Erskine-Smith (Beaches—East York, Lib.): D'abord, merci beaucoup.

J'aimerais d'abord parler du bulletin opérationnel PRG-2015-31 « Examination of Digital Devices... », l'inspection des appareils électroniques... Ce sont des lignes directrices provisoires, et je comprends l'inquiétude en ce qui concerne le fait qu'elles ont été communiquées en raison d'une demande d'accès à l'information et qu'elles n'ont pas été transparentes comme elles auraient dû l'être depuis le début. Je reconnais qu'elles n'ont pas officiellement force de loi; c'est un aspect que nous aimerions peut-être étudier. Je comprends tout à fait le témoignage de l'ACLU quant aux importantes lacunes qui existent au chapitre des mesures de protection de la vie privée aux États-Unis à l'heure actuelle.

Outre la question du mot de passe, expliquez-moi ce qui ne va pas avec ces lignes directrices provisoires.

La question s'adresse à l'ALCCB et à l'ACLC.

Je vais commencer avec Micheal.

Mme Micheal Vonn: Bien sûr. La première chose qui cloche avec les lignes directrices provisoires tient au fait que nous ne savons pas si elles sont suivies. Elles n'ont pas force de loi. Ce sont des guides. Nous espérons qu'elles sont utilisées, mais nous ne savons pas si c'est réellement le cas et nous n'avons aucun moyen de les appliquer si elles ne le sont pas.

M. Nathaniel Erskine-Smith: À cet égard, supposons que nous recommandons qu'elles aient force de loi. Leur libellé est-il un problème? Je veux en venir à la question de la protection du mot de passe et à la capacité de forcer des gens à révéler leurs mots de passe, mais je vais mettre ce sujet de côté pour le moment. Y a-t-il d'autres aspects des lignes directrices qui vous dérangent?

Mme Micheal Vonn: En ce qui concerne le libellé, il est question « d'indices ». Nous aimerions voir ce terme traduit par ce que nous considérons comme la langue juridique normalisée; on lirait donc « motifs de soupçonner », probablement à cet égard.

M. Nathaniel Erskine-Smith: J'ai une question à ce sujet.

J'ai devant moi les lignes directrices. En réalité, elles renvoient à des lois. Par exemple, au paragraphe 139(1) de la Loi sur l'immigration et la protection des réfugiés, il est question de motifs « raisonnables »; il existe donc un seuil établi en vertu de la LIPR. Selon la Loi sur les douanes, le document d'orientation laisse entendre que des « fouilles peuvent être menées s'il y a des indications que l'appareil pourrait contenir la preuve d'infractions. » Y a-t-il des préoccupations à l'égard de ce libellé vague?

Mme Micheal Vonn: Oui. Il faudrait préciser ce que cela signifie du point de vue des normes juridiques.

M. Nathaniel Erskine-Smith: Ce qui me frappe, c'est que l'ASFC a probablement mal interprété la loi en premier lieu. Si on observe l'alinéa 99(1)a), il est absurde de penser qu'il s'applique aux téléphones cellulaires, mais si on lit l'alinéa 99(1)f), on y trouve de meilleurs motifs pour fouiller des marchandises, et en fait, il énonce les critères de « motifs raisonnables ».

Vous ne les avez pas devant vous, mais seriez-vous d'accord pour que l'ACLC et l'ALCCB y jettent un oeil et évaluent si l'alinéa 99(1) f) a du sens? Il énonce les motifs raisonnables de la loi. Peut-être qu'au lieu de réécrire les dispositions, nous pourrions simplement préciser qu'il s'agirait de la source de la fouille. À mes yeux, l'alinéa 99(1)a) est tout à fait illogique. Par exemple, on peut y lire que l'agent peut « prélever des échantillons en quantités raisonnables ». Comment cela pourrait-il s'appliquer à un téléphone cellulaire qui n'a pas été importé en bonne et due forme?

Ma deuxième question concerne les mots de passe. Dans les lignes directrices, on peut lire que les agents peuvent « demander le mot de passe » et « ce ne doit pas être dans le but d'avoir accès à tout type de compte... sauvegardé en ligne ». En fait, il semble que l'appareil devrait être en mode avion ou quelque chose comme ça. On peut aussi lire que, si le « voyageur refuse de fournir un mot de passe... l'appareil... peut être confisqué ». Je crois comprendre qu'il y a eu un cas d'accusation d'obstruction, et qu'une personne a plaidé coupable et a payé une amende de 500 $. Mais, j'ai remarqué une tournure plutôt étrange dans les lignes directrices: on pouvait lire « jusqu'à nouvel ordre ». Selon elles, on ne peut arrêter un voyageur pour motifs d'obstruction ni porter d'accusations contre lui après-coup.

Selon l'ALCCB, quel serait le libellé approprié en ce qui a trait à la protection du mot de passe à la frontière si ce n'est pas celui-ci?

● (1725)

Mme Micheal Vonn: Je vais devoir étudier la question et je serai en mesure de répondre au Comité. Je ne l'ai pas à l'esprit pour le moment...

M. Nathaniel Erskine-Smith: Ça va. Voilà une meilleure utilisation de mes cinq minutes en fait. Si l'ALCCB et l'ACLC pouvaient fournir un mémoire au sujet de leurs préférences au sujet de la gestion des mots de passe à la frontière, ce serait excellent.

L'autre aspect à préciser dans les lignes directrices, si on les dissèque, est le suivant. Les lignes directrices de l'ASFC mentionnent aussi clairement, en ce qui a trait à la fouille en vertu de l'alinéa 99(1)a) de la Loi sur les douanes, qu'elles s'appliquent aux fins des douanes uniquement, donc l'idée selon laquelle on procède à des fouilles à très grande échelle pour d'autres motifs ne tiendrait pas nécessairement la route. Ce que je veux dire, c'est que je crois comprendre qu'il faut codifier cette pratique d'une meilleure façon dans la loi. Je suis frappé par le fait que ce soit déjà considérablement codifié dans la Loi sur les douanes et la LIPR; dans la mesure où nous pouvons faire mieux, c'est très bien. Mais j'aimerais savoir ce qui ne va pas avec les lignes directrices et le préciser le plus possible.

Je pense que j'ai vraiment dépassé mon temps. Voilà pour mes questions. Merci beaucoup.

Le président: Merci, monsieur Erskine-Smith.

Si vous me le permettez, j'aimerais poser quelques petites questions à Me Bhandari.

Lorsqu'un voyageur traverse la frontière, les agents des douanes américains peuvent-ils faire la distinction entre des données qui ont été volontairement mises dans le téléphone par l'utilisateur et des données qui ont été diffusées dans le téléphone sans intervention volontaire; il peut même s'agir de renseignements non souhaités? Y a-t-il des lignes directrices à cet égard?

Mme Esha Bhandari: Certainement pas dans la politique rendue publique, et je n'ai rien vu qui permettait d'établir une telle distinction que ce soit dans des recommandations ou dans une politique.

Le président: Y a-t-il une politique ou des lignes directrices qui concernent les données qui peuvent se retrouver dans le nuage, compte tenu du fait qu'il existe de nombreux forfaits de données et d'échange de données qui incluent de multiples appareils appartenant à de multiples utilisateurs au sein d'une même famille, d'une entreprise ou d'un groupe qui échange des renseignements dans le nuage? Y a-t-il des lignes directrices que devraient connaître les Canadiens?

Mme Esha Bhandari: Il n'y a aucune ligne directrice ni même de référence à cet égard dans la politique de 2009. Nous avons entendu parler — de façon empirique, encore une fois — de personnes qui ont vu leurs comptes de médias sociaux fouillés, et ça ne tenait vraisemblablement pas compte du fait que les renseignements étaient communiqués à d'autres personnes ou non.

Le président: Qui était responsable de la surveillance des critères à appliquer pour l'élimination ou la suppression de l'information lorsqu'il n'y avait aucun motif valable?

Mme Esha Bhandari: Des préoccupations ont été exprimées au Bureau de l'inspecteur général au département de la Sécurité intérieure.

On a mené il y a plusieurs années une évaluation de l'impact sur les libertés civiles au cours de laquelle on a examiné les pratiques et tenté de déterminer si les lignes directrices de la politique étaient respectées. Ce sont là certaines des mesures que prennent les défenseurs des droits, et bien sûr les gens peuvent parfois déposer des plaintes administratives, avec plus ou moins de succès.

Le président: Savez-vous s'il y a déjà eu un incident au cours duquel le téléphone d'un étranger, ou plus précisément celui d'un Canadien, a été confisqué par des agents des douanes des États-Unis et n'a pas été retourné au propriétaire alors qu'aucune accusation n'avait été portée?

Mme Esha Bhandari: Je n'ai été informée d'aucun incident du genre.

● (1730)

Le président: Merci beaucoup.

J'aimerais remercier tous nos témoins d'avoir été patients.

Chers collègues, j'aimerais prendre deux minutes pour passer à huis clos afin de discuter d'affaires du Comité pour la semaine prochaine.

J'aimerais remercier l'Association canadienne des libertés civiles, l'Association des libertés civiles de la Colombie-Britannique et l'American Civil Liberties Union de leur patience aujourd'hui.

N'hésitez pas à nous faire part de toute préoccupation que vous pourriez avoir ou de toute réponse écrite concernant certaines des questions qui ont été posées.

Chers collègues, nous allons suspendre la séance. Nous allons poursuivre à huis clos durant environ deux minutes.

[*La séance se poursuit à huis clos*]