



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 066 • 1^{re} SESSION • 42^e LÉGISLATURE

TÉMOIGNAGES

Le lundi 18 septembre 2017

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

Le lundi 18 septembre 2017

• (1555)

[Traduction]

Le vice-président (M. Nathaniel Erskine-Smith (Beaches—East York, Lib.)): Bon retour de vacances à tous. Nous tenons aujourd'hui la 66^e séance du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, qui poursuit son étude sur la protection des renseignements des Canadiens aux postes frontaliers et aux États-Unis.

Dans le cadre de cette étude, nous recevons aujourd'hui des représentants du Commissariat à la protection de la vie privée du Canada, soit M. Therrien, commissaire à la protection de la vie privée, Mme Ives, directrice générale par intérim, Vérification et revue, et Mme Kosseim, avocate générale principale et directrice générale, de la Direction des services juridiques, des politiques, de la recherche et de l'analyse des technologies.

Vous avez la parole.

M. Daniel Therrien (commissaire à la protection de la vie privée du Canada, Commissariat à la protection de la vie privée du Canada): Je vous remercie de m'avoir invité à comparaître devant vous aujourd'hui dans le cadre de votre étude sur la frontière.

Il faut examiner en contexte la question du droit à la vie privée à la frontière, compte tenu de l'importance que le commerce revêt, bien entendu, pour le Canada. Cela signifie que des mesures de contrôle bien pensées s'imposent pour les biens et les données qui traversent la frontière.

L'un des sujets signalés pour les besoins de votre étude a trait aux vérifications et aux fouilles effectuées par les agents des services frontaliers canadiens. Comme vous le savez, ces agents possèdent de vastes pouvoirs; ils peuvent interroger les voyageurs, recueillir des renseignements biométriques à des fins d'identification et examiner, fouiller ou retenir des biens, quels qu'ils soient.

En ce qui concerne la fouille de personnes, les agents peuvent procéder à une fouille par palpation ou sommaire, prendre une radiographie ou faire un balayage corporel. Ils peuvent même exiger une fouille à nu ou un examen des cavités corporelles. Toute fouille de personnes nécessite des motifs raisonnables de soupçonner une infraction quelconque, notamment la dissimulation de biens ou de toute autre chose qui pourraient représenter une menace à la vie ou à la sécurité de quiconque.

De leur côté, les appareils électroniques sont traditionnellement considérés comme des biens par l'Agence des services frontaliers du Canada. En vertu des alinéas 99(1) a) et c) de la Loi sur les douanes, l'agent peut examiner et ouvrir toute marchandise, et en prélever des échantillons sans motif. Ces dispositions s'appliquent à la fois aux marchandises qui entrent au Canada et à celles qui en sortent. De

plus, selon la jurisprudence relative à la *Charte canadienne des droits et libertés*, les autorités fédérales bénéficient d'une plus grande marge de manoeuvre à la frontière pour assurer la souveraineté et l'intégrité territoriale et contrôler l'immigration.

Parallèlement, la Cour suprême du Canada a aussi conclu dans de nombreux autres contextes que la fouille d'un appareil électronique est une procédure extrêmement envahissante. Ainsi, même si le droit n'est pas bien établi, il m'apparaît clair que les tribunaux canadiens considéreraient que les fouilles sans motifs sont inconstitutionnelles, même si elles sont faites à la frontière.

Le concept voulant que les appareils électroniques devraient être considérés comme de simples marchandises faisant l'objet de fouilles sans aucun motif juridique à la frontière est clairement dépassé et ne cadre pas avec les réalités de la technologie d'aujourd'hui. C'est peut-être bien pour cette raison que la politique du Canada est plus nuancée que la Loi sur les douanes.

Selon la politique de l'ASFC, il doit exister des motifs précis pour effectuer des fouilles, à savoir « que les appareils ou les supports numériques pourraient contenir des preuves de contraventions ». Je pense qu'il s'agit d'une politique avisée, mais qu'il faudrait en faire une règle de droit dans un avenir rapproché.

Une autre question importante reliée à la frontière concerne le projet de loi C-23, qui est actuellement devant le Sénat. Le projet de loi C-23, Loi sur le précontrôle, mettrait en oeuvre l'Accord entre le gouvernement du Canada et le gouvernement des États-Unis d'Amérique relatif au précontrôle dans les domaines du transport terrestre, ferroviaire, maritime et aérien conclu en 2015. Ce projet de loi prévoit que les agents des services frontaliers canadiens et américains exerceraient des activités de précontrôle à différents points d'entrée des deux côtés de la frontière.

J'ai exprimé des préoccupations lorsque l'administration américaine a annoncé son intention de fouiller les appareils électroniques de tout étranger qui veut entrer aux États-Unis. Ces fouilles seront exécutées à sa discrétion et sans aucun autre motif que la volonté d'assurer la sécurité nationale de façon générale.

Selon le projet de loi C-23, les contrôleurs américains au Canada sont assujettis au droit canadien dans l'exercice de leurs fonctions ou de leurs pouvoirs. Le gouvernement du Canada nous rappelle qu'ils seraient notamment assujettis à la *Charte canadienne des droits et libertés*, à la *Déclaration canadienne des droits* et à la *Loi canadienne sur les droits de la personne*. Toutefois, ces protections sont en quelque sorte futiles, puisqu'elles seraient sérieusement limitées par le principe de l'immunité des États, c'est-à-dire qu'elles ne pourraient être appliquées par une cour de justice.

Sachez qu'en vertu du projet de loi C-23, les contrôleurs américains au Canada doivent avoir des « motifs raisonnables de soupçonner » pour effectuer la fouille de personnes, y compris la fouille par palpation qui est relativement moins intrusive. J'estime que la fouille d'appareils électroniques peut être beaucoup plus envahissante que ces fouilles physiques.

• (1600)

Comme je le recommandais dans le cadre de l'étude du projet de loi C-23, les fouilles d'appareils électroniques à la frontière devraient s'effectuer pour des motifs raisonnables de soupçonner une infraction à la loi, un seuil qui serait similaire à celui s'appliquant aux fouilles des personnes.

[Français]

Le printemps dernier, je vous ai informés de ma correspondance avec trois ministres du gouvernement au sujet de certains décrets présidentiels de la nouvelle administration américaine. Des mesures comme celles-ci ont clairement une incidence importante sur la vie privée de plusieurs citoyens, étant donné l'importance du tourisme et des voyages d'affaires vers les États-Unis.

Un de ces décrets exclurait explicitement de certaines mesures de protection de la vie privée les personnes qui ne sont pas des citoyens américains ni des résidents permanents reconnus aux États-Unis.

Après examen, j'ai conclu que la vie privée des Canadiens bénéficie d'une certaine protection aux États-Unis, mais que cette protection est précaire, car elle repose principalement sur des engagements ou des ententes administratives qui ne sont pas exécutoires, notamment l'accord du Groupe des cinq et l'accord Par-delà la frontière conclu avec les États-Unis.

J'ai donc exhorté les représentants du gouvernement fédéral à demander à leurs homologues américains de renforcer la protection de la vie privée offerte aux Canadiens. Cela pourrait se faire, par exemple, en ajoutant le Canada à la liste des pays désignés en vertu de la Judicial Redress Act des États-Unis. De cette façon, certaines protections prévues par cette loi s'appliqueraient aux Canadiens, comme elles s'appliquent aux citoyens de plusieurs pays européens.

Nous avons aussi demandé au gouvernement de nous donner l'assurance que la protection offerte par les ententes administratives canado-américaines sera maintenue en dépit du décret et de nous informer de tout changement qui pourrait porter atteinte à la vie privée des Canadiens. Nous savons que les résultats de ces démarches ont maintenant été compilés et qu'une réponse sera disponible prochainement.

Passons maintenant aux ententes en matière d'échange d'information avec les États-Unis.

De façon générale, au cours des dernières années, nous avons consacré beaucoup de temps aux enjeux liés à la frontière et à l'échange d'information, en particulier aux initiatives menées conjointement avec les États-Unis dans le cadre du plan d'action Par-delà la frontière. À ce jour, nous avons fait des commentaires sur une cinquantaine d'évaluations des facteurs relatifs à la vie privée portant sur ces seules initiatives. Dans ces échanges, nous avons formulé une série de recommandations à l'ASFC et à d'autres ministères fédéraux qui cherchaient à élargir l'échange d'information et d'autres procédures à la frontière.

De façon générale, nous sommes satisfaits de l'ampleur des consultations et de la qualité accrue des analyses des facteurs relatifs à la vie privée entreprises par les organismes chargés de la sécurité à la frontière.

Cela dit, nous avons encore des préoccupations concernant les périodes de conservation applicables aux données recueillies auprès des voyageurs et le risque que les données recueillies aux fins de douane soient ensuite utilisées à d'autres fins.

Ces deux enjeux, à savoir la conservation des données et leur utilisation secondaire, ont été jugés problématiques du point de vue du droit européen dans une récente décision de la Cour de justice de l'Union européenne sur la ratification de l'Accord entre la Communauté européenne et le gouvernement du Canada sur le traitement des données relatives aux informations préalables sur les voyageurs et aux dossiers passagers.

En conclusion, étant donné que les gens, les biens et les données traversent les frontières avec une fréquence accrue, il est important que le Parlement s'assure d'instaurer des règles appropriées afin de respecter la vie privée des individus. L'importance de ces règles a été reconnue historiquement à l'égard de la fouille des personnes. Selon moi, le temps est venu d'étendre ces protections aux appareils électroniques.

Merci de votre invitation. Cela me fera plaisir de répondre à vos questions.

• (1605)

[Traduction]

Le vice-président (M. Nathaniel Erskine-Smith): Merci beaucoup.

Nous commencerons le tour de questions de sept minutes avec M. Saini.

M. Raj Saini (Kitchener-Centre, Lib.): Bonjour, monsieur Therrien. Je vous remercie de témoigner avec vos collègues. Je blaguais avec vous. Je pense que vous êtes presque un membre permanent du Comité, puisque vous comparez au moins une fois par mois. J'espère que vous avez autant profité de l'été que nous.

M. Daniel Therrien: J'ai effectivement passé un bel été.

M. Raj Saini: Maintenant que nous sommes ici, je veux vous poser une question quelque peu technique, car certains événements se sont produits au printemps. La Federal Communications Commission a modifié certaines des règles régissant les fournisseurs de service Internet, alors même que Trump adoptait un décret, de sorte qu'un Canadien se présentant à la frontière américaine pourrait se voir demander le mot de passe de son appareil. Sa vie privée n'est donc pas protégée. En outre, à un moment donné, il pourrait connecter son téléphone ou un autre appareil à Internet, et ses données pourraient être vendues en vertu des règles de la FCC.

Pouvez-vous me donner une idée de ce que vous pensez de la situation? Quels conseils auriez-vous à ce sujet? Quelle incidence ces changements auront-ils au Canada?

M. Daniel Therrien: Voilà des questions qui couvrent beaucoup de matière.

M. Raj Saini: Vous disposez de sept minutes.

Des voix: Ah, ah!

M. Daniel Therrien: Bien entendu, la première chose à dire, c'est que les États sont souverains, y compris les États-Unis d'Amérique. Ainsi, comme je l'ai indiqué dans mon exposé, j'ai demandé au gouvernement du Canada de prendre certaines mesures pour protéger la vie privée des Canadiens, tout d'abord en élaborant des lois appropriées pour protéger les renseignements de nature fort délicate que renferment les appareils électroniques en vertu du droit canadien, et, dans la mesure du possible, en s'intéressant à l'accord de précontrôle.

Mais à un moment donné, un Canadien qui souhaite se rendre aux États-Unis, que ce soit à des fins de tourisme ou d'affaires ou pour un autre motif, se retrouvera devant les autorités américaines, et les États-Unis sont libres d'adopter les règles qui sont dans leur intérêt afin de protéger leur sécurité. Cela signifie apparemment que les agents des services frontaliers américains... En mettant de côté le précontrôle, si un Canadien veut aller aux États-Unis et se retrouve devant un agent des services frontaliers, que ce soit à un poste frontalier terrestre ou à un aéroport américain, il pourrait devoir fournir le mot de passe de son téléphone cellulaire.

Je ne pense pas que cette pratique protège la vie privée, mais le gouvernement américain a le pouvoir d'imposer cette règle. Nous pourrions discuter ce qui constitue une approche prudente de la part d'un Canadien en pareille situation, mais vous vous penchez actuellement sur les lois et les pratiques des États-Unis. Ce pays est compétent et a le pouvoir d'imposer ses règles. Je ne pense pas qu'elles soient bonnes, mais ce sont celles qui seront apparemment imposées aux voyageurs.

Vous faites entrer en jeu le point de vue du secteur privé en évoquant les modifications du FCC afin de savoir si les renseignements recueillis par le gouvernement américain pourraient être vendus. Je n'ai pas analysé la question en détail. Ce qui est certain, c'est qu'à la suite du décret du président Trump qui a limité, voire éliminé la protection des personnes qui n'ont pas la citoyenneté américaine, les Canadiens nous ont bien entendu fait part de leurs préoccupations. Nous nous sommes penchés sur la situation pour déterminer s'ils étaient protégés. Aucune loi ne les protège, mais il existe un certain nombre d'accords administratifs qui, jusqu'à leur abrogation, leur offrent une certaine protection. Parmi ces mesures administratives de protection figure un décret pris par l'ancien président Obama qui assure une protection similaire aux non-Américains en ce qui concerne les activités de la National Security Agency, particulièrement en ce qui a trait à l'utilisation que le gouvernement américain fait des renseignements qu'il intercepte au nom du service de renseignement étranger.

Je vous donne les grandes lignes des règles qui sont applicables. Il reste encore des mesures administratives de protection aux États-Unis. Bien entendu, étant des mesures administratives, elles peuvent être abrogées demain par l'administration américaine, mais pour l'instant, il reste encore des mesures de protection pour les citoyens canadiens.

• (1610)

M. Raj Saini: J'ai une dernière question, que je rendrai légèrement plus facile.

Nous savons que le Règlement général sur la protection des données entrera en vigueur en mai 2018. Nous savons également que contrairement à nous, les États-Unis et l'Europe sont dotés d'un bouclier de protection de la vie privée et que l'Union européenne en arrivera à demander à tous ses membres de hausser leur niveau avec l'entrée en vigueur du règlement.

Pensez-vous qu'au lieu que les États-Unis et l'Union européenne aient une norme alors que le Canada est dépourvu de protection en raison du décret, il serait prudent ou probablement plus facile qu'ils adoptent tous une même norme?

M. Daniel Therrien: Cela faciliterait certainement les choses, mais c'est un fait bien connu qu'il existe des différences substantielles entre les approches des États-Unis et de l'Europe au chapitre de la protection de la vie privée. Je ne pense pas que cela arrivera dans un proche avenir, ce qui, de toute évidence, place le Canada dans une position difficile.

J'ai demandé à ce que certaines mesures de protection juridique soient offertes aux Canadiens. Par exemple, le fait de demander au gouvernement américain d'ajouter le Canada à une liste de pays à qui la protection est offerte en vertu de la Judicial Redress Act ne serait pas la même chose que d'avoir un régime tripartite, mais nous pouvons agir. Ce que je veux dire, c'est que nous pouvons prendre des mesures sans aller jusqu'à instaurer un régime tripartite entre l'Union européenne, les États-Unis et le Canada.

M. Raj Saini: Pourriez-vous nous donner brièvement un exemple de pays figurant sur la liste de recours judiciaire?

M. Daniel Therrien: Un bon nombre de pays européens, soit plus de 20, y figurent, essentiellement en raison des pressions que les États européens ont exercées sur les États-Unis au cours des échanges qu'ils ont eus avec eux et qui ont mené à l'adoption du bouclier de protection de la vie privée. Toutes ces questions sont interconnectées, et ce n'est pas par bonté de cœur que les États-Unis ont inscrit certains États européens sur cette liste: c'est en raison des pressions que ces derniers ont exercées sur eux. Le Canada pourrait adopter cette approche.

Le vice-président (M. Nathaniel Erskine-Smith): Merci beaucoup.

Sur ce, nous débuterons notre deuxième tour de questions de sept minutes.

Monsieur Kent, bienvenue parmi nous.

L'hon. Peter Kent (Thornhill, PCC): Merci beaucoup, monsieur le président. C'est un plaisir d'être avec vous.

Merci beaucoup, monsieur le commissaire, madame Kosseim et madame Ives, de témoigner aujourd'hui.

Comme nous et la majorité des Canadiens le savons, la manière d'effectuer des vérifications et des fouilles varie grandement d'un agent à l'autre et d'un endroit à l'autre, selon qu'il s'agit de précontrôle aérien, terrestre ou maritime.

Avez-vous des statistiques sur les plaintes relatives aux trois sortes de contrôles en ce qui concerne l'interrogatoire et les procédures entre un poste frontalier terrestre, un poste de précontrôle à l'aéroport Pearson ou un terminal maritime d'arrivée et de départ de navires touristiques?

M. Daniel Therrien: Je peux entreprendre de vous donner les chiffres. Je ne les ai pas avec moi en ce moment, mais nous ne recevons pas beaucoup de plaintes à cet égard. Les annonces faites il y a quelques mois au sujet des nouvelles pratiques du gouvernement américain quant aux appareils cellulaires en ont suscité quelques-une. Avant l'arrivée de ces pratiques, nous avons reçu moins de 10 plaintes à propos de problèmes à la frontière. Nos tendances ne s'appuieront donc pas sur un grand nombre de plaintes.

• (1615)

L'hon. Peter Kent: Il s'agirait pour la plupart d'observations empiriques ou d'affaires ayant paru dans les médias.

M. Daniel Therrien: Oui.

L'hon. Peter Kent: Bien souvent, quand nous voyageons dans d'autres pays à titre de parlementaires, on nous conseille de laisser nos appareils personnels à la maison et d'emporter un dispositif jetable ne contenant que les renseignements que nous serions prêts à partager avec les gens de ces pays.

Conseilleriez-vous aux Canadiens de réfléchir, par mesure de prudence, aux renseignements que renferment leurs appareils avant de partir en voyage d'ici à ce que nous ayons une meilleure idée de la manière dont les choses se passeront?

M. Daniel Therrien: Je conseillerais certainement aux Canadiens de limiter le nombre d'appareils qu'ils emportent aux États-Unis, et d'examiner et de restreindre les renseignements qu'ils renferment. Je considère qu'il serait prudent de voir si vous pouvez laisser au Canada, sur des appareils locaux, un ordinateur personnel ou autre chose, les renseignements que vous souhaitez conserver et dont vous n'avez pas besoin aux États-Unis.

Si vous avez besoin de renseignements à des fins professionnelles aux États-Unis, comme des informations protégées par le secret professionnel de l'avocat ou un autre privilège juridique au Canada, et que vous ne voulez pas que les agents des services frontaliers américains les examinent, vous pouvez les téléverser dans une section sécurisée du nuage, par exemple, afin de pouvoir y accéder une fois aux États-Unis. En bref, réfléchissez bien au genre de renseignements que vous voulez emporter avec vous dans vos appareils électroniques quand vous traversez la frontière, car vous savez que les agents des services frontaliers américains peuvent les exiger. Il serait prudent d'agir en conséquence.

L'hon. Peter Kent: À titre de parlementaires, nous avons des appareils dotés de niveaux de sécurité différents, outre la prise d'empreinte digitale ou le mot de passe requis pour accéder aux niveaux généraux. Considéreriez-vous ici encore que les parlementaires ou les gens d'affaires du secteur privé sont aussi vulnérables que les simples citoyens qui ont peut-être des niveaux de sécurité secondaire, voire des mesures de cryptage, et que les agents des services frontaliers pourraient leur demander aussi de leur donner accès à ces autres niveaux?

M. Daniel Therrien: Selon ce qu'a annoncé l'administration américaine, les agents peuvent exiger les renseignements contenus dans les appareils sans le moindre motif juridique, simplement pour une volonté compréhensible de protéger la sécurité nationale. Cette mesure s'applique à tous, sans égard aux dispositifs de sécurité dont les appareils sont dotés. Les agents considèrent que si vous entrez aux États-Unis, ils peuvent exiger votre mot de passe ou le déverrouillage de tout dispositif de sécurité les empêchant d'accéder aux renseignements qu'ils souhaitent consulter.

L'hon. Peter Kent: Vous avez fait référence à la période de conservation et à la décision de la Cour européenne de justice. Cette dernière s'est-elle penchée sur la conservation en général ou s'est-elle intéressée à la différence entre les données du GPS, du répertoire téléphonique ou de la messagerie textuelle?

M. Daniel Therrien: La Cour européenne a examiné un programme très précis, soit une ébauche d'accord entre le Canada et l'Union européenne sur le transfert de certains genres de renseignements sur les voyageurs entre ces deux régions. Son étude portait précisément sur ces informations, bien que des leçons puissent être tirées d'autres programmes de contrôle frontalier. La décision elle-même concernait ce programme précis.

L'hon. Peter Kent: Je vois.

Pour terminer, j'ai une très brève question. Vous avez indiqué que le gouvernement vous a assuré qu'une réponse s'en venait au sujet de l'assurance que vous lui avez demandé de vous fournir. À quelle réponse vous attendez-vous?

● (1620)

M. Daniel Therrien: Le gouvernement m'a indiqué que les États-Unis lui avaient communiqué certaines informations et qu'il nous les ferait parvenir bientôt.

L'hon. Peter Kent: Merci.

Le vice-président (M. Nathaniel Erskine-Smith): Sur ce, nous accorderons la parole à M. Cullen.

M. Nathan Cullen (Skeena—Bulkley Valley, NP): Merci, monsieur le président.

Je suis ravi de vous revoir également, monsieur Therrien.

J'aborde cette question du point de vue d'un profane, ce qui est en fait un avantage dans ce cas-ci. Pour le grand public canadien, c'est-à-dire les voyageurs qui souhaitent se rendre aux États-Unis, il faut définir les attentes. Vous nous avez dit aujourd'hui que les Canadiens devraient savoir qu'il est tout à fait possible et légitime qu'un agent des douanes américain demande à obtenir le contenu de tout appareil électronique qui franchit la frontière.

M. Daniel Therrien: En vertu de la loi, oui.

M. Nathan Cullen: C'est exact. Par conséquent, aucun Canadien qui traverse la frontière avec un téléphone, un ordinateur portable ou une tablette ne devrait se sentir à l'abri de ces intrusions.

M. Daniel Therrien: En effet, d'un point de vue juridique. Évidemment, la frontière ne pourrait pas être gérée de manière efficace si tout le monde était fouillé, mais légalement, je dirais que oui.

M. Nathan Cullen: Très bien. N'empêche que je songe aux répercussions politiques. Je ne peux même pas m'imaginer une telle situation, mais supposons que notre ministre du Commerce, un sous-ministre ou un fonctionnaire se rend à la frontière américaine, ordinateur portable en main, en vue d'aller négocier l'ALENA, et que notre stratégie se trouve dans cet ordinateur, ou supposons qu'il s'agit d'un sous-ministre adjoint qui s'en va négocier un accord commercial important. En vertu de cette loi, compte tenu des vastes pouvoirs conférés aux organismes frontaliers, le contenu de cet ordinateur portable, notamment notre stratégie, pourrait être divulgué.

M. Daniel Therrien: Sous réserve des relations diplomatiques.

M. Nathan Cullen: D'accord, sous réserve des relations diplomatiques. Cela pourrait provoquer un tollé, mais du point de vue juridique, c'est tout à fait légitime.

M. Daniel Therrien: Absolument.

M. Nathan Cullen: D'accord.

Je regardais la liste des pays désignés, c'est-à-dire la liste des pays que les Américains ont jugé suffisamment sécuritaires pour bénéficier des mêmes protections en vertu de la loi américaine sur la protection des renseignements personnels. La Pologne, le Portugal, la Roumanie, la Slovaquie, la Slovénie, l'Espagne, la Suède, l'Italie, la Lettonie, la Lituanie, le Luxembourg — tous ces pays ont pu obtenir une certaine protection pour leurs citoyens en vertu de la loi sur la protection des renseignements personnels des États-Unis, alors qu'il semble que le Canada n'ait pas cherché à obtenir cette même protection ou n'a pas été en mesure de l'obtenir. Est-ce exact?

M. Daniel Therrien: La raison pour laquelle les États-Unis ont désigné des pays sur cette liste n'a pas tant à voir avec la protection de l'information. En fait, c'est plutôt le contraire. Les Européens disposent de lois très strictes en matière de vie privée et ils ont exercé des pressions sur le gouvernement américain afin qu'il protège l'information de leurs citoyens au moment où ils traversent la frontière américaine — la Pologne, etc. — faute de quoi ils refuseraient de communiquer de l'information aux États-Unis.

M. Nathan Cullen: Je reviens donc à ma question. Le Canada a-t-il demandé ou non des protections semblables pour les citoyens canadiens?

M. Daniel Therrien: J'ignore si le gouvernement canadien en a fait la demande, mais c'est certainement quelque chose qu'il pourrait faire.

M. Nathan Cullen: Chose certaine, si l'Estonie a pu obtenir une protection pour ses citoyens qui voyagent en Amérique, je ne crois pas que c'est un conflit commercial avec ce pays qui a amené les États-Unis à se ranger de ce côté. En tant que leur plus important partenaire commercial, on s'attendrait à avoir plus d'influence dans ce type de conversations.

M. Daniel Therrien: Le fait que nous sommes un important partenaire commercial des États-Unis est évidemment un facteur qui entre en ligne de compte.

M. Nathan Cullen: Au-delà du public voyageur, les gens d'affaires qui voyagent et qui ont des entreprises aux États-Unis... D'accord. C'est intéressant.

Vous avez dit plus tôt, en réponse à la question de mon collègue, que les Canadiens devraient limiter le nombre de dispositifs qu'ils apportent en voyage. C'est la recommandation officielle de votre bureau à l'intention des voyageurs: N'apportez pas tout ce que vous avez, et ce que vous apportez... Peut-être devrions-nous recourir à des téléphones cellulaires jetables, dans ce cas-ci, pour éviter de laisser des traces? Généralement, les Canadiens se servent de ce type de téléphone pour avoir des frais de téléphone cellulaire moins élevés lorsqu'ils sont aux États-Unis.

Dans cette optique, me recommanderiez-vous de ne pas apporter mon téléphone du travail lorsque je vais aux États-Unis?

M. Daniel Therrien: Cela dépend de votre seuil de tolérance face au risque que vos renseignements fassent l'objet d'une vérification par les agents des douanes américaines. Il y a donc une évaluation personnelle à faire. Par exemple, si des renseignements confidentiels se trouvent sur votre appareil, à ce moment-là, vous avez une responsabilité accrue de les protéger. Selon moi, vous devez songer aux conséquences auxquelles vous vous exposez si cette information est divulguée et limiter la quantité de renseignements que vous apportez aux États-Unis, étant donné que les agents des douanes peuvent en faire l'acquisition.

•(1625)

M. Nathan Cullen: Et qu'ils peuvent les communiquer. Cela ne se limite pas qu'aux agents des douanes. Si on se fie à la façon dont fonctionne le régime de sécurité américain, la communication est... Je me souviens d'un concitoyen...

M. Daniel Therrien: Les renseignements pourraient être communiqués.

M. Nathan Cullen: Un de mes concitoyens s'est vu refuser l'entrée aux États-Unis, car de l'information personnelle sur son téléphone a révélé qu'il prenait des médicaments pour le cœur, et l'agent a conclu qu'il présentait un risque élevé de crise cardiaque. Je considère que c'est une intrusion assez étrange dans la vie privée

d'une personne qui veut simplement aller en vacances dans un autre pays. Ces renseignements ont ensuite été communiqués à une agence de la santé américaine.

Un autre de mes concitoyens n'a pas pu entrer aux États-Unis, car un agent des douanes a mis la main sur une ordonnance qui révélait qu'il prenait des médicaments pour traiter le sida.

M. Daniel Therrien: C'est possible.

Nous avons reçu une plainte il y a quelque temps. Cela n'avait rien à voir avec les appareils électroniques, mais une personne s'est fait interdire l'entrée aux États-Unis sous prétexte qu'elle avait déjà appelé le 911 au cours d'un épisode difficile. La personne avait songé au suicide, et c'est la raison pour laquelle on lui a refusé l'accès aux États-Unis. Cela ressemble un peu à l'exemple que vous avez donné d'une personne qui ne peut pas entrer aux États-Unis en raison de son état de santé.

M. Nathan Cullen: J'ai une dernière question. Est-ce que l'enquête doit toujours être physique? Je ne suis pas un technologue. Est-ce que l'organisme frontalier peut extraire les données du téléphone à distance, lorsque je traverse la frontière? Nous avons pris connaissance des pratiques d'espionnage à l'aéroport Pearson à Toronto où les appels entrants et sortants faisaient l'objet d'une surveillance.

Doit-il toujours y avoir une intervention physique, ou est-ce que cela peut se faire autrement? Est-ce que nous le savons?

M. Daniel Therrien: Si ce n'est pas physique, vous vous trouvez dans un territoire visé par l'interception des communications, ce qui comporte différentes règles.

M. Nathan Cullen: Merci.

Le vice-président (M. Nathaniel Erskine-Smith): Merci beaucoup, monsieur Cullen.

Sur ce, je vais céder les sept dernières minutes à M. Long.

M. Wayne Long (Saint John—Rothesay, Lib.): Merci, monsieur le président, et bienvenue à tous les nouveaux membres du Comité. Je suis ravi de voir de nouveaux visages autour de la table.

M. Nathan Cullen: Vous en aviez assez des vieux visages?

M. Wayne Long: Je n'ai pas dit cela.

Encore une fois, monsieur le commissaire, je vous remercie d'être des nôtres aujourd'hui. Vous comparez régulièrement devant le Comité, et nous vous sommes reconnaissants pour votre contribution.

J'aimerais commencer en vous racontant une situation que j'ai vécue il n'y a pas très longtemps à la frontière. Je représente la circonscription de Saint John—Rothesay, qui est située à une heure de la frontière de Calais. Lorsque nous sommes arrivés au poste frontalier, on nous a demandé de sortir de la voiture pour aller à l'intérieur discuter avec les agents des douanes. On m'a ensuite demandé de retourner à la voiture en compagnie d'un des agents afin d'y déposer nos téléphones ouverts. Je suis ensuite retourné à l'intérieur et nous avons dû attendre 30 à 45 minutes. J'étais accompagné d'un ami, de mon fils et d'une autre personne. On nous a finalement dit que tout était beau et que nous pouvions retourner à la voiture. À notre arrivée, nous avons constaté que les téléphones n'étaient pas au même endroit où nous les avions laissés.

Comme M. Cullen l'a dit, c'est une source de préoccupation lorsqu'on traverse la frontière. Évidemment, comme vous dites, ils ne sont pas obligés de nous laisser entrer aux États-Unis. Cependant, du point de vue d'un Canadien — et encore une fois, je suis désolé, j'abonde dans le même sens que M. Cullen.

Dans quelle mesure les Canadiens devraient-ils être préoccupés? Comme M. Cullen l'a dit, nous voyageons maintenant avec nos tablettes, nos ordinateurs portatifs et nos téléphones, et toutes mes finances personnelles et mes courriels se trouvent dans mon téléphone. On ne parle pas ici que de messages ou de photos. Tous mes dossiers et l'historique de ma vie entière s'y trouvent. Par conséquent, sur une échelle de 1 à 10, dans quelle mesure les Canadiens devraient-ils être inquiets?

M. Daniel Therrien: Comme vous le dites, ces appareils renferment de grandes quantités de renseignements de nature délicate. Nous devrions être très préoccupés. La loi permet aux agents américains de recueillir tous les renseignements qu'ils veulent, car il n'y a pas de motifs d'ordre juridique pour justifier leurs actions. Pour être réaliste, j'ai établi la distinction avec M. Cullen entre la loi et la pratique. Les agents des douanes ne disposent pas des ressources et ne peuvent pas passer en revue le contenu des appareils de tous les voyageurs qui traversent la frontière. Dans un certain sens, c'est un élément du contexte, mais il reste qu'en principe, je pense qu'il est juste de dire que ces appareils renferment de grandes quantités de renseignements très personnels, de nature très délicate. Lorsque la loi, y compris la loi canadienne, continue de traiter le contenu des appareils cellulaires comme étant des marchandises, des boîtes de carton ou des vêtements, c'est tout simplement irréaliste.

•(1630)

M. Wayne Long: Très bien.

Sur le site Web du Commissariat à la protection de la vie privée, il y a une rubrique intitulée « Votre droit à la vie privée dans les aéroports » qui explique comment nous devrions avoir des attentes moins élevées. J'ai lu dans ce même document d'information que l'on recueille le nom, la date de naissance, le sexe, la nationalité, l'information figurant sur les documents de voyage, l'itinéraire, l'adresse, l'information sur le paiement du billet, l'information pour grands voyageurs, les détails relatifs aux bagages et les numéros de téléphone pour — évidemment — évaluer les risques liés à la sécurité.

Pouvez-vous nous faire part de ce que vous en pensez? Ces renseignements sont-ils détruits de façon appropriée? Combien de temps sont-ils stockés? Le sont-ils de façon appropriée? Est-ce que l'on s'attend à ce que ces renseignements recueillis soient conservés? Une entente a-t-elle été conclue avec nous? Pouvons-nous revenir et dire, « Écoutez, vous conservez ces données pendant un mois », ou peuvent-ils être conservés pour toujours?

M. Daniel Therrien: Vous parlez des renseignements recueillis à propos des voyageurs par les douaniers canadiens?

M. Wayne Long: Oui.

M. Daniel Therrien: La conservation des données est de toute évidence une question importante, mais je vais commencer par dire qu'il est légitime pour les douaniers canadiens et, du reste, pour les douaniers américains de recueillir des renseignements personnels afin de déterminer si la personne qui veut entrer dans le pays peut le faire. Par conséquent, je ne soutiens pas qu'aucune donnée ne devrait être recueillie. Il est raisonnable de colliger certains renseignements pour pouvoir prendre une décision concernant l'admission. Mais si certains éléments d'information sont raisonnablement liés à la décision d'admettre une personne ou non au pays, ce qui nous

préoccupe, c'est combien de temps ils sont conservés — vous avez le droit de soulever cette question — et à quelle fin ils peuvent être divulgués à d'autres ministères.

M. Wayne Long: Qu'est-ce qui est acceptable? Quelle durée serait appropriée? Six mois? Une semaine?

M. Daniel Therrien: Tout dépend de la raison pour laquelle on recueille les renseignements. Si, par exemple, les renseignements sont recueillis pour déterminer la légalité de votre statut au Canada, alors je pense qu'il est juste de les conserver jusqu'à ce que l'on ait déterminé si vous êtes au pays légalement ou illégalement. Tout dépend de la raison pour laquelle les renseignements sont colligés. Ils sont principalement recueillis pour des raisons de gestion des frontières, alors il n'y a pas qu'une seule réponse possible concernant la durée. Tout dépend de la raison pour laquelle ils sont colligés, et si c'est pour une bonne raison, combien de temps le gouvernement doit-il les conserver pour atteindre ce qu'ils cherchent à atteindre?

M. Wayne Long: Merci.

Le vice-président (M. Nathaniel Erskine-Smith): Excellent.

Sur ce, nous allons passer à M. Gourde, pour cinq minutes.

[Français]

M. Jacques Gourde (Lévis—Lotbinière, PCC): Merci, monsieur le président. Je suis heureux de me joindre à votre comité.

Je remercie les témoins d'être présents.

Monsieur Therrien, croyez-vous que la fréquence des vérifications d'appareils électroniques faites à la douane augmente? Est-ce fait seulement de façon aléatoire?

M. Daniel Therrien: Parlez-vous du Canada ou des États-Unis?

M. Jacques Gourde: Je parle des États-Unis.

M. Daniel Therrien: Aux États-Unis, une augmentation a été remarquée. Selon les données recueillies, les appareils cellulaires ont fait l'objet de fouilles 5 000 fois en 2015 et 25 000 fois en 2016. Il s'agit donc d'une augmentation de 500 % de 2015 à 2016. De plus, selon des chiffres fiables pour 2017, il y a eu 5 000 fouilles en un seul mois, soit en février 2017. Il y a donc une augmentation.

•(1635)

M. Jacques Gourde: Vos statistiques nous permettent-elles de détecter si certains groupes sont plus ciblés que d'autres? Y a-t-il plus de fouilles aléatoires, ou cela touche-t-il surtout les personnes plus jeunes ou encore les personnes plus âgées?

M. Daniel Therrien: Ces chiffres ont été colligés par d'autres personnes que nous. Ce sont donc des chiffres que nous avons pu voir. À ma connaissance, on ne fait pas de distinction selon les groupes. Ce serait évidemment une question pertinente à poser.

M. Jacques Gourde: Je crois que cela fait partie des préoccupations d'un bon nombre de Canadiens.

Les douaniers canadiens font-ils la même chose? Vérifient-ils des appareils électroniques d'Américains qui viennent au Canada?

M. Daniel Therrien: Comme je l'expliquais lors de mon allocation, le droit canadien permet beaucoup de choses aux douaniers. En droit canadien, les appareils cellulaires sont traités comme des biens. À ce titre, ils peuvent faire l'objet de fouilles sans motif, à l'heure actuelle. C'est le droit statutaire.

La politique du gouvernement canadien et de l'Agence des services frontaliers du Canada est de restreindre cette capacité juridique, de façon à ce que les appareils en question ne puissent faire l'objet de perquisitions ou de fouilles que si le douanier canadien a des motifs de soupçonner que quelque chose est lié à une contravention quelconque.

La politique est donc moins permissive, à mon avis, que le droit, parce que le gouvernement et l'Agence des services frontaliers du Canada pressentent que les tribunaux ne valideraient pas l'utilisation de pouvoirs sans motif comme le droit statutaire le permet.

M. Jacques Gourde: Si un Canadien se plaint parce que son appareil électronique a été fouillé et que, par conséquent, des informations industrielles, de brevet ou autres ont été perdues, existe-t-il un recours pour lui, ou ces informations sont-elles perdues à tout jamais?

M. Daniel Therrien: Même si l'information est colligée et recueillie par le gouvernement en fonction de ses pouvoirs, cela ne lui donne pas le droit d'utiliser les renseignements à des fins illégitimes.

Si le gouvernement prend possession de certains renseignements, il y a un risque évident, mais le Canada ne pourrait divulguer ou utiliser ces données comme bon lui semblerait. Une faute serait certainement commise si des secrets industriels étaient divulgués, sauf s'il y avait une autorisation judiciaire ou légale de le faire.

M. Jacques Gourde: Des Canadiens ont-ils déjà porté plainte relativement à cette situation?

M. Daniel Therrien: Nous avons reçu un petit nombre de plaintes et, en effet, nous sommes en train d'enquêter sur celles-ci. Cela porte sur la fouille d'appareils cellulaires par l'Agence des services frontaliers du Canada.

M. Jacques Gourde: Si ce sont des Canadiens qui se plaignent de douaniers américains, est-ce que leur recours est limité?

M. Daniel Therrien: Si un Canadien se présente sur le territoire américain et demande à y être admis, non, il n'a aucun recours.

Cependant, un amendement au projet de loi C-23, qui est présentement à l'étude au Parlement, a été suggéré par le Comité permanent de la sécurité publique et nationale afin que les Canadiens qui se présentent à une zone de précontrôle aient accès à un mécanisme administratif de gestion de la frontière, à défaut d'avoir accès à un tribunal. À mon avis, ce n'est pas suffisant, mais c'est une amélioration qui a été apportée à la mouture originale du projet de loi.

M. Jacques Gourde: Pensez-vous qu'il pourrait y avoir une entente réciproque?

[Traduction]

Le vice-président (M. Nathaniel Erskine-Smith): Il pourrait nous rester du temps à la fin pour poser plus de questions.

Je vais accorder les cinq prochaines minutes à Mme Fortier.

[Français]

Mme Mona Fortier (Ottawa—Vanier, Lib.): Merci beaucoup, monsieur le président.

Monsieur Gourde, je suis contente que vous ayez commencé à poser des questions sur les plaintes, parce que je veux aussi comprendre ce qu'il en est.

Quel type de plaintes recevez-vous? J'ai compris que vous en aviez reçu quelques-unes. Comment déterminez-vous si elles sont

valables dans le contexte actuel? Y a-t-il une tendance qui se dégage de ces plaintes?

M. Daniel Therrien: Au cours des derniers mois ou de la dernière année environ, nous avons reçu trois plaintes sur ces pratiques. En vertu de la Loi sur la protection des renseignements personnels, nous avons l'obligation légale d'étudier chaque plainte. Ce ne sont pas toutes les plaintes qui doivent être étudiées avec la même rigueur, mais il reste que nous devons toutes les étudier.

Comme il y a seulement trois plaintes, il est difficile de voir si une tendance s'en dégage. Je peux dire cependant qu'il s'agit certainement de gens qui ont lu dans les médias ou dans différentes annonces que leurs appareils risquaient d'être fouillés par les autorités canadiennes ou américaines. Des gens sont préoccupés de cela à juste titre et veulent s'assurer que les pratiques du gouvernement sont légales. Ils nous ont donc adressé des plaintes, que nous sommes en train d'examiner.

• (1640)

Mme Mona Fortier: Avec la nouvelle loi proposée, croyez-vous être en mesure de traiter de la même façon les plaintes que vous pourriez recevoir de Canadiens et de Canadiennes? De quel genre de plaintes s'agirait-il?

M. Daniel Therrien: Parlez-vous de la Loi sur le précontrôle?

Mme Mona Fortier: Oui, justement.

M. Daniel Therrien: Si un Canadien voit son appareil cellulaire ou électronique fouillé par un douanier américain en sol canadien en vertu de ce régime, nous n'avons pas compétence. Ce sont les autorités américaines qui ont compétence, selon l'entente entre le Canada et les États-Unis.

Le seul mécanisme qui permettrait à une personne de s'adresser à un Canadien, c'est ce qui a été proposé par le Comité permanent de la sécurité publique et nationale par l'entremise de l'amendement au projet de loi dont je viens de parler.

Mme Mona Fortier: Vous avez parlé de ce qui se faisait en Europe. Y a-t-il des pratiques exemplaires dont nous pourrions nous inspirer pour améliorer la proposition que nous faisons présentement?

M. Daniel Therrien: Parlez-vous de la gestion de la frontière au Canada plutôt que du côté des États-Unis?

Mme Mona Fortier: J'aimerais savoir si nous pourrions nous inspirer des pratiques d'ailleurs pour nous assurer que les Canadiens et les Canadiennes sont davantage protégés quant à leurs appareils électroniques.

M. Daniel Therrien: Le droit européen est rigoureux quant aux principes d'ordre général. Le jugement de la Cour de justice de l'Union européenne où il était question du programme à la frontière nous a permis de le constater. À ma connaissance, le droit européen traite de ces questions selon de grands principes. Il considère en effet que, de façon générale, les ministères et les gouvernements peuvent recueillir des renseignements uniquement lorsque c'est nécessaire et proportionnel au but visé. À ma connaissance, il n'y a pas de règle très précise quant à l'application de ces grands principes dans le contexte de la douane. Cela dit, nous pourrions faire une vérification à ce sujet.

À mon avis, ce qui est en cause ici, c'est le fait qu'il y ait au Canada, en ce qui concerne l'étendue des pouvoirs des douaniers à la frontière, une longue lignée jurisprudentielle qui dit que, à la frontière, l'attente en matière de vie privée est moindre que dans d'autres contextes, étant donné que la personne demande à être admise dans un autre pays. Je crois que ce principe demeure vrai. Toutefois, celui-ci a été utilisé de façon à ce que les garanties juridiques à la frontière soient extrêmement limitées, sinon inexistantes.

L'avènement des appareils électroniques fait en sorte qu'il faut se poser des questions. Les douaniers ont le droit de faire certaines fouilles à la frontière, mais cela devrait-il aller jusqu'à fouiller dans les dossiers financiers se trouvant dans un téléphone, dans les informations au sujet des relations intimes ou de l'état de santé d'une personne, par exemple? Poser la question, c'est y répondre. Il faut que le Canada arrive en 2017 et traite juridiquement ces appareils comme il se doit.

Mme Mona Fortier: Merci.

[Traduction]

Le vice-président (M. Nathaniel Erskine-Smith): Merci beaucoup.

Nous allons maintenant entendre M. Zimmer pour les cinq prochaines minutes.

M. Bob Zimmer (Prince George—Peace River—Northern Rockies, PCC): Merci. Je suis ravi de faire partie du Comité. Je suis l'un des membres les plus récents ici. Merci de nous accueillir parmi vous. C'est une bonne entrée en matière.

Monsieur Therrien, nous avons discuté dans le passé. Nous avons déjà participé aux travaux des comités. Nous avons abordé les questions de l'accès à l'information, du piratage, de la sécurité des appareils, etc. J'imagine que ce qui nous a ouvert les yeux entre autres — et je ne me souviens pas de la date exacte où vous étiez ici —, c'est lorsque nous discutons de ce dont nous savons au sujet des pirates d'aujourd'hui. Ce sont des jeunes du secondaire qui sont à la maison et qui recueillent des renseignements pour le plaisir. Ce sont des organisations criminelles qui veulent mettre la main sur nos renseignements. C'est ce sur quoi je vais fonder ma question.

Quels sont les pires abus concernant les renseignements auxquels vous faites allusion? Qu'avez-vous constaté comme utilisation ou abus d'information à la frontière? Y a-t-il des liens avec le crime organisé? Le crime organisé a-t-il eu accès à ces renseignements qu'il cherche à obtenir? Ce lien a-t-il déjà été établi?

•(1645)

M. Daniel Therrien: Je n'ai pas été témoin de cas de cette nature, mais je vais vous dire ceci. Ce que la loi autorise essentiellement à l'heure actuelle, c'est la collecte de données dans l'intérêt de la sécurité à la frontière. Les criminels et les pirates potentiels constituent un facteur pertinent à considérer. Je ne veux pas exagérer la nature du problème, mais plus le gouvernement collige des renseignements, plus le risque de piratage à des fins criminelles augmente, de toute évidence. Je pense que c'est une autre raison pour laquelle le gouvernement devrait faire attention de ne pas recueillir des renseignements au-delà de ce qui est nécessaire, et même si c'est nécessaire, il ne devrait pas les conserver au-delà de la durée requise. Le gouvernement est évidemment un dépositaire de grandes quantités de renseignements très intéressants pour des personnes qui nourrissent des intentions criminelles.

M. Bob Zimmer: Pour revenir à ma question, avez-vous vu des exemples? Vous ne pouvez peut-être pas évoquer tous les exemples

devant un comité public. Avez-vous été témoin d'exemples où des données ont été colligées, comme dans le cas que M. Cullen a mentionné, où une personne s'est vu refuser l'entrée au pays parce qu'elle souffrait d'un problème de santé? De là à qualifier cette situation d'abus n'est peut-être pas approprié, mais quel est le pire abus attribuable à la collecte de données que vous avez vu? En tant que commissaire à la protection de la vie privée, pouvez-vous nous donner quelques exemples d'effets négatifs découlant de la collecte de ces données?

M. Daniel Therrien: Il n'y en a pas eu beaucoup, mais il y en a eu quelques-uns, et par quelques-uns, je ne parle pas de renseignements recueillis au moyen d'appareils.

L'exemple qui me vient à l'esprit est celui d'une femme dont les renseignements ont été colligés par un service de police au Canada durant une crise qu'elle traversait, une tentative de suicide, où elle a composé le 911. Cette information est versée dans les dossiers de la police, qui est ensuite communiquée aux autorités frontalières américaines à des fins de coopération entre les organismes d'application de la loi au Canada et aux États-Unis. Les agents américains ont pris la décision de refuser l'entrée au pays à la dame parce qu'ils estimaient qu'elle était à risque de s'enlever la vie ou de mettre en danger la vie de citoyens américains.

Cette situation est survenue à cause de l'appel au 911, mais la même chose pourrait se produire lors d'une fouille d'un appareil électronique qui révélerait la présence d'une maladie, par exemple.

M. Bob Zimmer: Merci.

Le vice-président (M. Nathaniel Erskine-Smith): Il vous reste 45 secondes, si vous voulez poursuivre.

M. Bob Zimmer: J'ai terminé. Merci.

Le vice-président (M. Nathaniel Erskine-Smith): Je regarde l'heure, et il nous restera du temps pour que tous les membres puissent poser leurs questions.

Le dernier intervenant de cette série de cinq minutes est M. Dubourg.

[Français]

M. Emmanuel Dubourg (Bourassa, Lib.): Merci, monsieur le président.

C'est à mon tour de saluer les témoins qui sont avec nous cet après-midi.

Monsieur Therrien, j'aimerais que vous parliez de l'échange d'information avec les États-Unis. Vous avez dit que le plan d'action Par-delà la frontière contient plusieurs recommandations, mais il n'en demeure pas moins que vous avez encore des préoccupations, d'abord en ce qui concerne la période de conservation des données. Quant à moi, c'est surtout l'autre partie qui m'intéresse, c'est-à-dire le risque que les données recueillies aux fins de douane soient ensuite utilisées à d'autres fins.

Dans un premier temps, j'aimerais savoir quel genre de fins vous aviez en tête lorsque vous avez écrit cela. Ensuite, j'aimerais savoir de quelle façon nous pouvons éviter que ces informations soient utilisées à d'autres fins.

•(1650)

M. Daniel Therrien: Mettons les choses en contexte. On parle ici de renseignements obtenus par le gouvernement canadien à la frontière qui seraient divulgués à d'autres ministères à d'autres fins que le contrôle de la frontière.

Le gouvernement canadien a rendu publique son intention d'utiliser ces renseignements à des fins d'intégrité des programmes, par exemple. Il veut ainsi pouvoir vérifier si quelqu'un prétendant être au Canada à des fins de résidence, ce qui lui procure certains avantages sociaux, y est réellement. C'est l'une des fins pour lesquelles le gouvernement voudra utiliser ces renseignements. Il peut également y avoir des fins d'ordre fiscal, ce qui pourrait donner lieu à un échange d'information avec les corps policiers, par exemple. Toutes ces fins sont envisageables. En fait, le gouvernement a indiqué son intention d'utiliser ces renseignements à de telles fins.

De notre côté, nous ne voulons pas nécessairement dire que ces fins sont inacceptables, mais nous voulons voir dans quelle mesure les différents ministères qui recevraient des renseignements de la douane en ont besoin aux fins de leurs programmes. Nous n'en sommes pas encore à cette étape et nous attendons des renseignements du gouvernement sous la forme d'évaluations des facteurs relatifs à la vie privée. Nous attendons certaines données du gouvernement, qui doit nous informer de façon plus détaillée sur la justification de ces fins.

M. Emmanuel Dubourg: D'accord.

La conservation de ces informations et l'accès à celles-ci par les ministères deviennent assez importants, puisque l'échange d'information est fait à l'insu de la personne.

Il y a autre chose. Il faut savoir si le ministère qui reçoit les renseignements a un processus de contrôle pour limiter l'accès des employés à ces renseignements.

M. Daniel Therrien: Pour ce qui est des périodes de conservation, je vais vous donner un exemple. Quand l'Agence des services frontaliers du Canada nous a consultés pour la première fois au sujet de certains de ces programmes, elle nous a informés vouloir conserver les renseignements pour une période de 75 ans. Ces consultations ont eu lieu il y a un certain temps. Nous en avons discuté avec l'Agence et elle a ensuite décidé de réduire cette période à 30 ans, de façon à pouvoir identifier les individus, et de dépersonnaliser les données après 15 ans.

Il y a un dialogue avec les ministères. On voit qu'il y a un désir de conserver les données pour une très longue durée. Après discussion, nous réussissons souvent à réduire la période de conservation, mais il est difficile d'avoir une discussion avec les ministères qui aille au fond des choses. Encore une fois, il n'y a pas de chiffre magique quant à la conservation. La vraie question est de savoir à quelles fins les ministères ont besoin de ces renseignements et combien de temps ils doivent les conserver pour pouvoir réaliser leurs objectifs, mais il est difficile d'avoir cette discussion avec eux.

M. Emmanuel Dubourg: En terminant, je présume que ces ministères ont un genre de période de grâce, si je puis dire. Par exemple, en matière d'impôts, une fois que la période des déclarations est terminée, on ne peut plus apporter de corrections ou émettre un nouvel avis de cotisation. Dans les autres ministères, il doit bien y avoir une période de trois, cinq ou dix ans de...

[Traduction]

Le vice-président (M. Nathaniel Erskine-Smith): Nous avons dépassé les cinq minutes imparties, alors soyez bref.

M. Daniel Therrien: Puis-je répondre à la question, en quelques secondes?

Le vice-président (M. Nathaniel Erskine-Smith): Nous avons dépassé les cinq minutes, alors répondez brièvement.

[Français]

M. Daniel Therrien: Tout ce que je dirais...

Ça va, j'ai perdu le fil.

Des voix: Ah, ah!

[Traduction]

Le vice-président (M. Nathaniel Erskine-Smith): C'était plus bref que prévu.

Voilà qui met fin à notre série d'interventions de cinq minutes. Nous aurons du temps plus tard, mais nous allons d'abord entendre M. Cullen, pour trois minutes.

• (1655)

M. Nathan Cullen: Merci encore une fois, monsieur le président.

Vos déclarations nous ont éclairés. J'ai l'impression que c'est un peu la combinaison de deux forces. L'une est l'environnement de sécurité vigoureux dans lequel nous évoluons depuis les 10, 15 ou 20 dernières années, certainement depuis le 11 septembre, et l'autre est la technologie extrêmement puissante et envahissante. Je me demande, à la lumière de vos discussions avec les Canadiens, ceux qui soulèvent des préoccupations ou déposent des plaintes officielles, s'il y a un manque de sensibilisation à l'égard de la situation, comme M. Long l'a signalé, de « Laissez vos téléphones dans la voiture et nous allons seulement y jeter un coup d'oeil », compte tenu de tous les renseignements que les cellulaires renferment — tous les mots de passe, les comptes bancaires et toutes les données personnelles.

Si un Canadien voyait un douanier fouiller tous ses bagages, sortir et parcourir tous ses effets personnels, ou fouiller sa maison, ce serait de toute évidence une atteinte à la vie privée. Ce sont ses effets personnels. Pourquoi fouiller dans les albums de photos des gens? Or, nous ne semblons pas avoir évolué au même rythme de la technologie existante et avoir pris conscience du pouvoir d'une personne lorsqu'elle dit, « J'ai besoin de votre téléphone et de votre mot de passe ».

J'imagine que c'est davantage une question philosophique, mais y a-t-il un délai de latence ou un retard que les Canadiens doivent rattraper pour savoir ce que c'est de traverser la frontière? Si nous recevions ce statut désigné, cela permettrait-il d'atténuer la majorité ou quelques-unes de vos préoccupations concernant les renseignements que nous fournissons lorsque nous entrons aux États-Unis?

M. Daniel Therrien: Il faut assurément du temps pour rattraper notre retard sur les nouvelles avancées en matière de sécurité et de technologie des dernières années, alors je dirais qu'il y a bel et bien un délai de latence — pour ce qui est de la compréhension des risques. Nous faisons de notre mieux pour informer les Canadiens par l'entremise des moyens que nous avons, mais je pense qu'il est également un peu déraisonnable et irréaliste de penser que les gens changeront complètement leur mode de vie pour ces raisons-là — et en Amérique du Nord, les déplacements sont nombreux entre le Canada et les États-Unis. Nous pouvons effectivement informer certaines personnes, et certaines personnes changeront leur comportement et n'apporteront pas autant de renseignements personnels, par exemple, mais le Parlement a un rôle très important à jouer pour s'assurer que les lois, dans la mesure où elles se rapportent aux agents canadiens, protègent les gens afin qu'ils ne fassent pas l'objet de fouilles sans motif.

M. Nathan Cullen: Je me demande si mes collègues ou moi émettons un bulletin ou un avis à nos concitoyens pour leur dire, « Si vous voyagez aux États-Unis, voici ce que le commissaire à la protection de la vie privée recommande: apportez quelques appareils et attendez-vous que les renseignements qui se trouvent dans ces appareils pourraient être remis, et ils peuvent l'être aux termes de la loi, à un agent américain ». Certains Canadiens pourraient trouver cette déclaration alarmiste. Ne pensez-vous pas?

M. Daniel Therrien: Fort possiblement, oui.

M. Nathan Cullen: C'est néanmoins ce que vous nous avez conseillé de faire.

M. Daniel Therrien: Oui.

Le vice-président (M. Nathaniel Erskine-Smith): Sur cette note optimiste, voilà qui conclut notre série d'interventions. J'ai quelques questions que j'aimerais poser, et je sais que M. Saini en a quelques-unes également.

Allez-y, monsieur Saini, puis nous passerons à M. Kent.

M. Raj Saini: Je veux seulement me prononcer sur quelques points que vous avez évoqués. Je veux obtenir quelques éclaircissements.

Vous avez dit qu'en 2016, 25 000 fouilles d'appareils cellulaires ont été effectuées aux États-Unis. D'après ce que j'ai lu dans le *New York Times*, il y a eu 383 millions d'arrivées aux États-Unis. Cela représente 0,0012 %. De ces 25 000 voyageurs qui ont fait l'objet de fouilles, y a-t-il moyen de savoir combien d'entre eux étaient des Canadiens? Dites-vous que 25 000 Canadiens ont fait l'objet de fouilles? Est-ce en général, pour que nous puissions avoir une idée des chiffres?

M. Daniel Therrien: Nous confirmerons plus tard, mais je crois que cette donnée représente le nombre de fouilles d'appareils électroniques appartenant à des non-Américains, et pas forcément à des Canadiens.

M. Raj Saini: Il n'y a donc pas de ventilation pour les Canadiens?

M. Daniel Therrien: Non.

M. Raj Saini: D'accord.

Je vais poser ma deuxième question pour m'assurer que je comprends bien. J'ai besoin de vos éclaircissements et de votre sagesse.

D'après ce que je comprends, le « bouclier vie privée » entre l'Union européenne et les États-Unis porte sur les renseignements qui sont envoyés par un organisme en Europe à un autre organisme aux États-Unis.

M. Daniel Therrien: Ou vice-versa...

M. Raj Saini: Mais il n'empêche pas, en aucune circonstance, un douanier américain de fouiller une personne provenant de ces pays qui voyage aux États-Unis.

M. Daniel Therrien: En effet.

• (1700)

M. Raj Saini: Nous discutons de deux choses différentes, n'est-ce pas?

M. Daniel Therrien: Cela ne change pas la loi américaine en ce qui a trait à ce que vous avez mentionné. Un douanier américain pourrait demander à un Européen de lui donner son mot de passe pour accéder au contenu de son appareil électronique. Les ententes entre les États-Unis et l'Europe offrent des recours à l'Européen dans ce cas-ci. Pour le Canada, puisque nous ne sommes pas un pays visé par la Judicial Redress Act, nous ne pouvons pas faire appliquer ces

mécanismes de recours. Le seul mécanisme qui pourrait être envisagé est celui que le comité SECU, le comité de la sécurité nationale, ajoute à l'accord relatif au précontrôle.

Essentiellement, les Européens sont assujettis aux mêmes fouilles aux États-Unis que les Canadiens, mais dans les faits, les Européens disposent d'un droit de recours que nous n'avons pas.

M. Raj Saini: Pouvez-vous nous expliquer plus en détail le droit de recours? En quoi consiste-t-il exactement?

M. Daniel Therrien: J'aimerais bien ne pas pouvoir le faire. Les États-Unis ont un ensemble assez complexe de mécanismes de recours, dont des recours à l'interne au gouvernement, comme des ombudsmans, par exemple, et des recours judiciaires. C'est un système compliqué.

M. Raj Saini: J'ai une dernière question. D'après ce que je comprends, lorsqu'un douanier canadien fouille le contenu d'un téléphone, ce téléphone doit être désactivé et ne peut pas être connecté à Internet et à un service en nuage. Est-il vrai que tout ce que l'on peut fouiller sur cet appareil est son contenu?

M. Daniel Therrien: Conformément à la politique de l'ASFC, oui.

M. Raj Saini: Du côté des États-Unis, ont-ils cette même capacité? La politique est-elle la même?

M. Daniel Therrien: Non. Les lois et les politiques américaines sont beaucoup plus permissives pour les douaniers. C'est différent. En vertu des politiques, les agents canadiens peuvent seulement fouiller le contenu de l'appareil, mais en vertu de la loi, ils pourraient aller beaucoup plus loin dans leur fouille.

Le vice-président (M. Nathaniel Erskine-Smith): Merci beaucoup.

Monsieur Kent, vous avez mentionné avoir une question complémentaire.

L'hon. Peter Kent: Oui. Elle fait suite à la question de M. Saini.

Vous avez dit plus tôt que si un voyageur qui se rend aux États-Unis, ou au Canada, voulait protéger et gérer ses données, il pourrait les stocker sur un nuage et y accéder une fois rendu à sa destination. Cela ne veut-il pas dire que les services de sécurité frontaliers, tant au Canada qu'aux États-Unis, sont quelque peu en retard? Il y a des gens qui ont des intentions criminelles ou malveillantes qui pourraient se soustraire à l'examen d'un appareil personnel et utiliser le nuage pour contourner le processus. À part l'idée naïve...

M. Daniel Therrien: Si des fonctionnaires d'un côté comme de l'autre de la frontière soupçonnent un individu d'être un criminel, ils peuvent faire appel à une autorité judiciaire pour obtenir ces renseignements, même s'ils sont stockés dans le nuage. La différence est que, pour obtenir ces renseignements qui seraient protégés par un criminel, il vous faudrait une autorisation judiciaire quelconque. À la frontière, c'est beaucoup plus facile.

L'hon. Peter Kent: Merci.

Le vice-président (M. Nathaniel Erskine-Smith): Avez-vous une question complémentaire?

M. Nathan Cullen: Je comprends mal les réponses aux questions de M. Saini et de M. Kent, car vous dites essentiellement qu'au Canada, nos organisations frontalières ne sont pas autorisées à saisir un appareil, à le fouiller puis à l'utiliser pour consulter l'information fonduagique de la personne. Vous avez toutefois dit qu'aux États-Unis, la loi et la pratique permettent aux autorités frontalières américaines d'accéder au nuage à l'aide d'un appareil. Or, vous aviez dit plus tôt que si les gens étaient inquiets, ils pourraient verser les renseignements commerciaux ou gouvernementaux sur le nuage, puis les récupérer une fois aux États-Unis. Me suivez-vous? J'ai peut-être mal compris, mais le conseil donné plus tôt semble être contraire à la réalité.

Disons que je vais aux États-Unis. Puisque j'ai des documents gouvernementaux de nature très délicate sur mon appareil, je les verse sur le nuage. Au moment de traverser la frontière, les agents demandent le mot de passe non seulement de mon téléphone, mais aussi du nuage, puisqu'ils en ont remarqué la présence.

M. Daniel Therrien: Aux États-Unis, les agents pourraient effectivement l'exiger.

M. Nathan Cullen: Par conséquent, le fait de verser l'information dans un nuage lorsque je vais aux États-Unis ne m'aidera en rien si j'ai des documents délicats que je préférerais garder hors de la portée des autorités frontalières américaines.

M. Daniel Therrien: Vous avez raison.

M. Nathan Cullen: Je voulais simplement que ce soit clair. Encore une fois, je rattrape mon retard sur le plan technologique.

Nous avons remarqué les décrets qui sont pris par l'administration actuelle. Quel a été le plus grand changement ayant affecté le public voyageur depuis l'élection du président Trump, en ce qui a trait aux enjeux que nous examinons aujourd'hui? Y a-t-il une différence majeure dans la façon dont l'information est traitée ou fouillée par rapport aux procédures de l'administration précédente, ou s'agit-il plus ou moins d'une suite logique?

• (1705)

M. Daniel Therrien: Nous n'avons pas étudié les pratiques de l'administration américaine. En réponse à la question, je dirais que le décret visant à limiter l'application de la Privacy Act des États-Unis envoie un message aux fonctionnaires américains selon lequel les données des ressortissants étrangers ne doivent pas être protégées. Il s'agit d'un message global. Ce qu'en font l'administration ou les fonctionnaires dépend des particularités de l'opération.

M. Nathan Cullen: Un message a donc été envoyé.

M. Daniel Therrien: En effet.

Le vice-président (M. Nathaniel Erskine-Smith): Je crois que M. Zimmer a une petite question à poser, après quoi j'en aurai quelques-unes.

M. Bob Zimmer: Je vous remercie encore une fois d'être avec nous. Vous avez parlé du démantèlement des données. Je connais bien les bases de données, et je sais qu'elles ne sont pas nécessairement détruites comme prévu. Comment pouvons-nous avoir la certitude que le gouvernement fédéral américain est sincère lorsqu'il dit vouloir conserver des renseignements précis pour une période donnée?

Comment pouvons-nous être certains que s'il dit que l'information a été supprimée, c'est bel et bien vrai? Je regrette de le dire publiquement, mais est-ce par simple respect à l'égard de l'autre pays que l'administration fera ce qu'elle a dit? Comment savons-nous si les données ont été entièrement détruites? Et que pouvons-nous faire

si nous soupçonnons que ce n'est pas le cas? Les Canadiens ont-ils des recours?

M. Daniel Therrien: C'est surtout une question de relations bilatérales entre les deux pays.

Le vice-président (M. Nathaniel Erskine-Smith): Merci.

En ce qui concerne la question de M. Cullen, je ferai remarquer que si j'ai sauvegardé des documents sur mon compte Google Drive, et que je n'ai pas l'application sur mon téléphone, je pourrai assurément traverser la frontière. Personne ne fouillera sur Google Drive, et j'y aurai accès aux États-Unis. Il faut alors supprimer l'application de son téléphone.

J'ai quelques questions. Tout d'abord, je suppose que vous faites référence au Bulletin PRG-2015-31 de l'Agence des services frontaliers du Canada, ou ASFC. Le document parle de la Loi sur les douanes et la Loi sur l'immigration et la protection des réfugiés, ou LIPR, et il expose l'orientation que les agents de l'ASFC doivent préconiser pour la fouille d'appareils électroniques.

Me Patricia Kosseim (avocate générale principale et directrice générale, Direction des services juridiques, des politiques, de la recherche et de l'analyse des technologies, Commissariat à la protection de la vie privée du Canada): Quel est le numéro?

Le vice-président (M. Nathaniel Erskine-Smith): C'est PRG-2015-31. Il s'agit de l'orientation stratégique qui dit que l'alinéa 99(1) a) de la Loi sur les douanes est uniquement à des fins douanières et s'applique en présence d'une multitude d'indices. Dans le cas de la LIPR, le paragraphe 139(1) fait référence à des motifs raisonnables; le but de la fouille doit se limiter à ces questions, et les agents doivent expliquer leur raisonnement. Certaines protections sont énoncées.

Je ne vous demande pas de le faire aujourd'hui, mais si vous pouviez examiner l'orientation préconisée par l'ASFC et voir si vous avez d'autres mesures de protection de la vie privée à y ajouter, il serait intéressant de remettre l'information à notre comité.

Je prends note de votre principal argument, à savoir que la politique est généralement juste, mais qu'elle doit être reprise dans les dispositions législatives. Nous devons d'abord recevoir vos propositions additionnelles, et vous recommandez ensuite que l'information se retrouve dans la loi de façon générale. On parle ici du côté canadien, si j'ai bien compris. Nous offrons des protections aux Canadiens et aux étrangers au moyen des règles de l'ASFC. Or, ces protections ne s'appliquent pas si nous voyageons aux États-Unis.

La représentante de la American Civil Liberties Union a témoigné devant nous, et elle a indiqué, tout comme vous, que les règles permettent au gouvernement de fouiller tout voyageur, peu importe sa citoyenneté, et tout appareil aussi sans mandat, motif probable, ni soupçon. Vous avez mentionné la Judicial Redress Act des États-Unis. Existe-t-il d'autres mesures ou mécanismes que nous devrions demander à nos homologues américains de mettre en place afin de protéger la vie privée des Canadiens, mis à part le simple fait d'ajouter le Canada à la liste des pays désignés aux termes de la JRA?

M. Daniel Therrien: J'ai demandé à trois de nos ministres de confirmer essentiellement que la protection conférée par les accords administratifs — et il y en a plusieurs — s'applique encore aux Canadiens malgré le message que le président Trump a envoyé dans son décret. Il faut notamment obtenir la confirmation du gouvernement américain que ces accords sont toujours en vigueur. C'est assurément une façon de procéder.

Le vice-président (M. Nathaniel Erskine-Smith): Avez-vous reçu une réponse affirmative de ces ministres?

M. Daniel Therrien: On me dit que le gouvernement canadien a obtenu de l'information du gouvernement américain, et que je la recevrai sous peu.

• (1710)

Le vice-président (M. Nathaniel Erskine-Smith): L'information sera-t-elle envoyée à notre comité aussi?

M. Daniel Therrien: Oui.

Le vice-président (M. Nathaniel Erskine-Smith): Nous vous serions reconnaissants de nous la faire parvenir dès que vous l'aurez en main.

M. Daniel Therrien: D'accord.

Il existe également un recours judiciaire aux États-Unis. Des citoyens américains contestent la nouvelle politique de leur pays, une question qui aboutira devant les tribunaux américains.

Le vice-président (M. Nathaniel Erskine-Smith): Avez-vous un homologue américain avec qui vous collaborez sur les enjeux relatifs à la vie privée? Je vous pose la question parce que la représentante de la American Civil Liberties Union a parlé d'une évaluation de la protection de la vie privée réalisée en 2005 par le département de la

Sécurité intérieure, où on semblait dire que le téléchargement et la reproduction des données des appareils électroniques survenaient déjà à la frontière. Je déteste devoir vous le dire, monsieur Long, mais tous les renseignements qui ont été examinés le sont peut-être encore, s'ils ont été reproduits.

Avez-vous un homologue américain avec qui vous collaborez et qui se penche sur ces enjeux aux États-Unis?

M. Daniel Therrien: Aux États-Unis, la structure du système est quelque peu différente, de sorte que je n'ai pas un seul homologue. Il y a cependant des spécialistes de la protection des renseignements personnels dans chaque ministère, y compris au département de la Sécurité intérieure, qui conseillent l'équipe sur les enjeux relatifs à la vie privée. Ces gens ne sont toutefois pas indépendants du pouvoir exécutif comme je le suis.

Le vice-président (M. Nathaniel Erskine-Smith): Merci beaucoup.

Vous nous avez donné matière à réflexion pour la formulation de nos questions en vue de notre visite aux États-Unis.

Y a-t-il d'autres questions? Dans le cas contraire, la séance est levée.

Publié en conformité de l'autorité
du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur*. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la *Loi sur le droit d'auteur*.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante : <http://www.noscommunes.ca>

Published under the authority of the Speaker of
the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its Committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its Committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act*. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act*.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the following address: <http://www.ourcommons.ca>