



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 016 • 2^e SESSION • 41^e LÉGISLATURE

TÉMOIGNAGES

Le mardi 1^{er} avril 2014

—
Président

M. Pat Martin

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

Le mardi 1^{er} avril 2014

•(1100)

[Traduction]

Le président (M. Pat Martin (Winnipeg-Centre, NPD)):
Bonjour, mesdames et messieurs.

Nous allons ouvrir la séance. Nous sommes ici aujourd'hui pour étudier le problème grandissant du vol d'identité et ses répercussions économiques. Nous sommes heureux d'entamer notre étude en compagnie de représentants du ministère de l'Emploi et du Développement social, MM. Louis Beauséjour et Robert Frelich. Ce premier groupe de témoins sera avec nous de 11 heures à midi, après quoi nous recevrons d'autres témoins.

Messieurs Beauséjour et Frelich, vous avez environ 10 minutes pour vos déclarations préliminaires et ensuite, nous permettrons aux membres du comité de poser leurs questions.

Monsieur, vous avez la parole.

[Français]

M. Louis Beauséjour (sous-ministre adjoint, Direction générale des services d'intégrité, Service Canada, ministère de l'Emploi et du Développement social): Monsieur le président, membres du comité, bonjour.

C'est avec plaisir que mon collègue Robert Frelich et moi comparaissons devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique.

Nous sommes heureux de vous fournir de l'information qui vous aidera à mener votre étude sur le problème croissant du vol d'identité et de ses répercussions économiques sur les citoyens et sur les entreprises ainsi que des mesures que peuvent prendre les entreprises et les organismes d'application de la loi pour protéger davantage les Canadiens et les Canadiennes.

Une de mes fonctions à titre de sous-ministre adjoint des services d'intégrité au sein de Service Canada est de mettre en place les processus et les mesures administratives liés à l'émission des numéros d'assurance sociale.

[Traduction]

Comme vous le savez peut-être, Service Canada est le volet de prestations des services au sein d'Emploi et Développement social Canada. Le ministère verse plus de 100 milliards de dollars chaque année dans le cadre de différents programmes et services, comme le programme d'assurance-emploi, le Programme canadien de prêts aux étudiants, le Régime de pensions du Canada et le Programme de la sécurité de la vieillesse. Et le numéro d'assurance sociale est utilisé dans l'ensemble de ces programmes.

Mais l'utilisation du numéro d'assurance sociale ne se limite pas à Emploi et Développement social Canada: en effet, de nombreux autres ministères et organismes fédéraux, comme l'Agence du revenu

du Canada, la GRC, l'Agence des services frontaliers et le ministère de la Justice se servent quotidiennement du NAS et du Registre d'assurance sociale, ou « RAS ».

Comme le NAS est un élément important qui permet de faire en sorte que la bonne prestation soit versée à la bonne personne au bon moment, il joue un rôle de premier plan dans la gestion de l'identité.

Aujourd'hui, je vous expliquerai comment nos pratiques d'attribution des numéros d'assurance sociale et l'administration du Registre d'assurance sociale se sont améliorées au fil des ans pour renforcer l'intégrité du programme des numéros d'assurance sociale et pour réduire l'incidence et l'impact de la fraude en matière d'identité.

L'évolution du programme des NAS peut être divisée en quatre périodes, du point de vue des mesures visant à renforcer l'intégrité du NAS et à mieux le protéger.

[Français]

La première période constitue ce que j'appelle les années initiales, qui vont de 1964 à 1976. La création du programme des NAS remonte à 1964, avec la mise sur pied d'un registre pour deux programmes fédéraux, soit le programme d'assurance-chômage, rebaptisé par la suite programme d'assurance-emploi, et le Régime de pensions du Canada.

Peu après, son utilisation a été étendue à l'Agence du revenu du Canada dans le cadre des déclarations de revenus. Depuis, le programme des NAS a été étendu davantage et utilisé comme indicateur unique pour plus de 50 programmes ou services fédéraux. Il constitue un élément incontournable dans la vie des Canadiens et des Canadiennes.

À l'époque, les mesures d'intégrité prévues dans le système d'émission des numéros d'assurance-sociale étaient très limitées. Par exemple, les employeurs étaient autorisés à demander l'émission de NAS pour leur employé. Les clients n'avaient pas à fournir de preuves d'identité et si quelqu'un avait perdu son NAS, un nouveau numéro pouvait lui être assigné.

La deuxième période va de 1976 à 1996. Je considère que, durant cette période, on a accru l'intégrité du système de traitement des demandes de NAS qui, à l'époque, se faisaient sur papier.

À partir du mois de juillet 1976, on a commencé à exiger que les clients fournissent des preuves d'identité et les demandes de NAS devaient être présentées par le client lui-même. De plus, les employeurs ne pouvaient plus faire la demande d'un NAS pour leur employé.

Au début, un grand nombre de documents d'identité étaient acceptés aux fins de l'émission des numéros d'assurance-sociale, y compris les pièces d'identité secondaires, comme des permis de conduire. Toutefois, à la fin de cette période, pratiquement plus aucun document secondaire n'était accepté et les agents se basaient sur des documents primaires comme des certificats de naissance et des documents émis par Citoyenneté et Immigration Canada.

● (1105)

[Traduction]

Durant la période allant de 1996 à 2006 nous avons commencé à faire la transition d'un système axé, dans une large mesure, sur une approche manuelle, sur support papier, vers un système dans lequel on commençait à inclure des mesures automatisées de protection de l'intégrité.

En novembre 1996, le premier de ces changements a été mis en oeuvre: l'établissement d'un lien électronique dans la base de données de Citoyenneté et Immigration Canada qui permettait de vérifier l'identité et le statut de résident permanent et de résident temporaire des personnes qui étaient arrivées au Canada après 1972.

En 1998, le Bureau du vérificateur général a commencé à s'intéresser de près au programme du NAS. Je vais prendre quelques instants pour vous faire part des différentes conclusions du bureau, car cette période fut charnière dans l'administration du NAS et du RAS.

Dans ses rapports de 1998 et 2002, le Bureau du vérificateur général notait principalement que les procédures de preuve d'identité devaient être améliorées, que les sources d'information existantes devaient être mieux utilisées, que les renseignements que contenait la base de données du NAS n'étaient pas toujours complets ni exacts, et qu'il y avait davantage de NAS en circulation que de Canadiens de plus de 20 ans.

En réponse à ces lacunes, d'importantes initiatives ont été lancées pour améliorer l'administration des NAS et du RAS, ce qui a contribué aux efforts faits par le gouvernement pour lutter contre le vol et la fraude liés à l'identité. Nous avons introduit l'indicateur inactif, ainsi qu'une date d'expiration pour les NAS émis aux travailleurs étrangers temporaires et nous avons créé un site Web de référence interne sur les preuves d'identité dans l'intranet.

[Français]

L'indicateur inactif identifie les NAS qui ne sont pas actifs depuis cinq ans consécutifs ou plus, c'est-à-dire les NAS à l'égard desquels il n'y a pas eu d'activité ayant trait au revenu, comme la présentation de déclaration de revenus ou des interactions avec des programmes gouvernementaux. Depuis lors, si quelqu'un a un indicateur inactif dans son dossier de numéro d'assurance sociale, il doit fournir une preuve d'identité originale pour réactiver son numéro d'assurance sociale, à savoir un certificat de naissance original s'il est né au Canada ou des documents de Citoyenneté et Immigration Canada, s'il est né à l'étranger.

Cette réactivation se fait en personne à un centre de Service Canada s'il réside au Canada, ou par la poste s'il réside à l'extérieur du Canada. De plus, pour aider les agents à mieux détecter les risques de fraude et de vol d'identité, on a développé en 2003 le site Web de référence interne des preuves d'identité ayant trait à l'émission des numéros d'assurance sociale dans l'intranet. Ce site Web donne aux agents responsables de l'émission des numéros d'assurance sociale un accès à des renseignements détaillés quant aux éléments à examiner dans les documents d'identité afin de s'assurer de leur authenticité.

En se fondant sur les recommandations visant à assurer une meilleure utilisation des sources d'informations, le ministère a signé des ententes avec les 10 provinces — en commençant par l'Ontario, en 2005 — afin de créer des liens électroniques entre les bureaux provinciaux de l'état civil et le Registre d'assurance sociale. Ces ententes nous permettent de valider l'information contenue dans les certificats de naissance émis par les provinces et d'obtenir des données concernant les décès, qui sont comparées ensuite aux données contenues dans le Registre d'assurance sociale. Cela nous permet de repérer les dossiers de personnes décédées et d'éviter ainsi que d'autres paiements leur soient versés par des programmes fédéraux.

De plus, ces ententes assurent l'intégration du système en permettant aux parents de faire la demande d'un numéro d'assurance sociale pour leur enfant au moment où ils enregistrent sa naissance auprès des autorités provinciales.

● (1110)

[Traduction]

Finalement, durant la période la plus récente, c'est-à-dire depuis 2006, le ministère a mis en place deux importants éléments pour faciliter l'administration des NAS: la formation et l'accréditation des agents et le Code de bonnes pratiques du numéro d'assurance sociale. Dans le contexte de notre programme d'accréditation, les agents suivent une formation portant tout particulièrement sur l'attribution et l'administration des numéros d'assurance sociale; depuis 2006, seuls les agents accrédités peuvent délivrer des NAS aux clients. Le Code de bonnes pratiques du NAS, qui est un document public disponible sur notre site Internet, renferme des normes et directives destinées aux utilisateurs du NAS — les citoyens canadiens, les employeurs et d'autres intervenants — afin qu'ils comprennent leurs responsabilités à l'égard du NAS.

[Français]

Par exemple, le code conseille les employeurs sur la façon de gérer l'information ayant trait aux employés, et particulièrement aux numéros d'assurance sociale. Il souligne le rôle clé que jouent les employeurs dans la détection et la prévention de la fraude liée aux numéros d'assurance sociale, étant donné que l'emploi illégal et la fraude fiscale sont deux des principales raisons à l'origine de ce type de fraude. Le code demande aux employeurs de signaler immédiatement à Service Canada tout abus soupçonné du numéro d'assurance sociale.

Nous avons commencé à recevoir les données concernant les naissances et les décès électroniques de l'Ontario en 2006.

La première province à avoir instauré la validation de l'information contenue dans les certificats de naissance était la Colombie-Britannique, en 2008. Actuellement, nous avons des liens électroniques avec huit provinces. Il est prévu que les liens avec les deux autres provinces seront établis d'ici 2016.

Nous sommes heureux de signaler que notre travail et nos efforts ont été reconnus par le Bureau du vérificateur général en 2009 et 2011. Il a en effet reconnu les mesures prises par le ministère en réponse aux préoccupations soulevées dans le cadre de vérifications antérieures et a précisé que le ministère avait apporté de considérables améliorations à cet égard.

[Traduction]

Maintenant, j'aimerais parler des deux initiatives les plus récentes visant à accroître l'intégrité du programme des NAS: le remaniement du traitement des demandes de NAS envoyées par courrier et l'élimination de la carte d'assurance sociale. Étant donné que les demandes de NAS envoyées par courrier représentaient seulement 4 % des 1,5 million de demandes traitées chaque année, qu'approximativement 55 % de ces requêtes étaient rejetées à cause d'erreurs dans les formulaires de demande et que les mesures de gestion de l'identité dans le contexte de l'envoi des demandes par la poste n'étaient pas aussi robustes que le traitement en personne, les demandes de NAS ne pourront plus être envoyées par courrier, sauf lorsqu'une personne habite dans une région éloignée, fait face à des restrictions en raison de circonstances atténuantes ou se trouve à l'étranger.

Le ministère était également conscient des problèmes d'intégrité causés par l'utilisation abusive de la carte d'assurance sociale. La carte d'assurance sociale n'était jamais censée être utilisée comme une carte d'identité, puisqu'elle ne contient pas des éléments de sécurité ou des caractéristiques distinctes. Cependant, en raison de son format réduit, un grand nombre des titulaires de la carte la conservait dans leur portefeuille, en dépit de la directive du ministère qui le leur déconseillait. À partir d'hier, les demandeurs ne recevront plus une carte d'assurance sociale, mais seront plutôt informés du NAS dans une lettre. Cette initiative aidera à empêcher le vol et la fraude liés à l'identité en cas de perte ou de vol des cartes d'assurance sociale.

[Français]

Le numéro d'assurance sociale est au coeur de l'administration de nombreux programmes. Depuis 1964, nous avons fait beaucoup de progrès pour créer un programme de numéro d'assurance sociale robuste qui aide les ministères et gouvernements à administrer le versement des prestations, tout en protégeant les clients contre le vol et la fraude liés à l'identité.

Nous travaillons continuellement avec les intervenants clés, en l'occurrence les autres ministères fédéraux, les provinces et territoires et le secteur privé, afin de déterminer les mesures que nous pouvons prendre pour réduire les risques de fraude et de vol liés à l'identité. Nous soumettons régulièrement nos processus et politiques à une évaluation pour les rendre plus sécuritaires et plus solides, et ce, afin de fournir des services de haut niveau aux Canadiens et Canadiennes.

Nous nous ferons maintenant un plaisir de répondre à vos questions, si vous en avez.

• (1115)

[Traduction]

Le président: Merci beaucoup monsieur Beauséjour.

Nous allons donc commencer immédiatement en cédant la parole à M. Mathieu Ravnignat de l'opposition officielle.

M. Mathieu Ravnignat (Pontiac, NPD): Merci, monsieur le président.

Merci à nos témoins d'être là.

Je pense que l'on peut dire sans hésiter que les Canadiens sont préoccupés par leurs renseignements personnels et que l'accès illicite à leurs données personnelles a augmenté depuis l'arrivée des divers médias sociaux. La loi existante n'est manifestement pas assez robuste ni assez moderne pour assurer la protection des Canadiens et

de leurs renseignements personnels. Je pense que l'appareil gouvernemental en souffre aussi quelque peu.

J'ai une question plus précise pour vous. Dans le rapport de la commissaire à la protection de la vie privée, déposé récemment, on peut trouver ce qui suit au paragraphe à la page 27:

Nonobstant ce qui précède, nous aimerions souligner que davantage de renseignements personnels que ceux signalés par EDSC aux personnes touchées pourraient avoir été compromis à la suite de la perte du disque dur.

Pouvez-vous nous expliquer pourquoi des renseignements personnels compromis n'ont pas été signalés précisément aux personnes touchées? Pourquoi le ministère a-t-il choisi de ne pas le signaler?

M. Louis Beauséjour: Je ne suis pas bien placé pour parler des détails de ces atteintes particulières, parce que je ne suis pas directement chargé du programme où cela s'est produit. À ma connaissance, nous avons agi très vite pour renseigner les clients, mais nous ne les avons pas renseignés sur les éléments clés d'information qui auraient pu se trouver sur le disque dur à ce moment-là.

M. Mathieu Ravnignat: Pourquoi pensez-vous alors que la commissaire a signalé que davantage de renseignements personnels n'ont peut-être pas été signalés aux personnes touchées?

M. Louis Beauséjour: Voulez-vous dire l'information qui aurait pu l'être? Je n'ai pas les détails avec moi.

M. Mathieu Ravnignat: Très bien. Ce serait bien si vous pouviez nous transmettre cette information parce qu'il est essentiel que les Canadiens, notamment les particuliers touchés, connaissent tous les types d'information qui ont été perdus dans ce cas-là et que...

Le président: J'allais justement, moi aussi, interrompre M. Ravnignat, mais allez-y.

Je vous permets de présenter votre rappel au Règlement.

M. Paul Calandra (Oak Ridges—Markham, PCC): Les témoins sont ici pour parler de vol d'identité, et non pas de ce rapport précis. Ils ne seraient donc absolument pas prêts à parler de ce rapport ni des atteintes à la sécurité des renseignements personnels.

Je suppose que nous pouvons certainement traiter de questions entourant la protection de l'identité, mais je ne suis pas certain de savoir si nous donnons aux témoins... Nous les mettons sur la sellette en leur demandant d'essayer de parler d'un rapport, alors que ce n'est pas la raison pour laquelle nous les avons invités ici.

Le président: Je vais traiter de cette question comme rappel au Règlement. Vous remettez en question la pertinence, je crois, et ce serait le seul argument que vous pourriez soulever dans le cadre d'un rappel au Règlement. Je déclare donc que votre objection est rejetée. Les questions de cette nature sont certainement pertinentes à notre sujet d'étude.

Toutefois, j'aimerais obtenir une précision. Monsieur Ravnignat, faites-vous référence à la perte ou au vol de dossiers de prêts étudiants parmi...

M. Mathieu Ravnignat: C'est exact, oui.

Le président: ... les 580 000 dossiers qui contiennent de l'information sur des prêts étudiants?

M. Mathieu Ravnignat: C'est exact, monsieur le président.

Le président: Je vous permets de poursuivre dans cette veine. J'estime qu'il ne s'agit pas d'un rappel au Règlement admissible légitime.

Monsieur Beauséjour, répondez du mieux que vous pouvez.

M. Mathieu Ravignat: Seriez-vous donc prêt à transmettre cette information au comité?

M. Louis Beauséjour: Le ministère vous transmettra l'information.

M. Mathieu Ravignat: Merci.

[Français]

Bien que le ministre de l'Emploi et du Développement social ait dit qu'il acceptait les recommandations de la commissaire à la protection de la vie privée, tel qu'indiqué dans le rapport, le demi-million de Canadiens qui ont été victimes de cette perte de données s'attendent à ce que leur gouvernement pose des gestes concrets.

Quelles mesures concrètes allez-vous prendre au cours des prochains mois pour répondre aux recommandations de la commissaire?

• (1120)

M. Louis Beauséjour: Comme nous l'avons précisé dans le rapport, nous avons déjà pris un certain nombre de mesures très concrètes pour répondre à ces recommandations.

[Traduction]

Au terme de l'incident, nous avons immédiatement réexaminé et renforcé notre procédure et notre protocole entourant la sécurité des technologies de l'information, surtout en ce qui avait trait à la manipulation des renseignements personnels sur des unités de stockage portatifs comme des clés USB et des disques durs externes.

Nous avons également pris des mesures pour renforcer la formation des employés relativement à la manipulation adéquate de données de nature délicate comme des renseignements personnels.

Plus précisément, nous avons instauré des protocoles plus rigoureux. Les disques durs externes non chiffrés ne sont plus permis au ministère.

[Français]

M. Mathieu Ravignat: Ces mesures étaient-elles en vigueur en 2013?

M. Louis Beauséjour: En réponse aux événements de 2013, nous les avons mises en vigueur immédiatement. Nous n'avons pas attendu les recommandations de la commissaire à la protection de la vie privée pour améliorer les mesures qui étaient en vigueur à ce moment-là, l'objectif étant de renforcer la protection des renseignements personnels.

M. Mathieu Ravignat: D'accord. Je vous remercie.

[Traduction]

Dans un monde numérique, il est important de réagir très rapidement lorsqu'il y a une perte d'information, en raison des conséquences, mais il a fallu attendre deux mois avant que ces incidents ne soient révélés.

Pouvez-vous m'expliquer pourquoi le délai a été aussi long?

M. Louis Beauséjour: Le ministère devait d'abord prendre un certain nombre de mesures. Il nous a fallu un peu de temps avant de nous rendre compte que le disque dur avait disparu. Ensuite, nous avons effectué un certain nombre de recherches dans l'édifice pour essayer de le trouver. Par la suite, il a aussi fallu du temps pour déterminer ce qui se trouvait précisément sur le disque dur. Nous sommes passés par toutes ces étapes entre le moment où nous avons pris connaissance du disque dur et celui où nous avons été en position de faire rapport.

Le président: Merci, monsieur Beauséjour. Nous allons devoir en rester là. Merci beaucoup.

Votre temps est écoulé, monsieur Ravignat.

Maintenant, M. Laurie Hawn va prendre la parole pour les conservateurs.

L'hon. Laurie Hawn (Edmonton-Centre, PCC): Merci, monsieur le président.

Merci à nos témoins de se joindre à nous.

J'aimerais ne pas m'attarder sur les dossiers égarés parce qu'il est difficile de déterminer si un nombre x de dossiers égarés, pour quelque raison que ce soit, auront tel ou tel résultat.

Pouvez-vous plutôt nous parler de la fréquence réelle des atteintes à la sécurité, c'est-à-dire de cas où quelqu'un s'est en fait servi du NAS de quelqu'un d'autre ou a utilisé son propre NAS à mauvais escient?

M. Louis Beauséjour: Nous ne sommes pas au courant de mauvaises utilisations du NAS à la suite d'un accès illicite donnant lieu à la perte de renseignements personnels.

L'hon. Laurie Hawn: Y a-t-il des cas d'utilisation illicite du NAS autre que...?

M. Louis Beauséjour: Oui, il y a quelquefois des cas d'utilisation frauduleuse du NAS. Dans le cadre de nos enquêtes régulières, nous faisons des examens liés aux prestations et, dans le cadre de ces examens, il se peut que nous découvrions des personnes utilisant frauduleusement un NAS pour obtenir des avantages.

L'hon. Laurie Hawn: Avez-vous une idée du nombre ou de la fréquence de tels cas?

M. Louis Beauséjour: Essentiellement, si l'on examine les chiffres du dernier exercice, nous avons mené plus de 4 500 enquêtes, aux termes desquels nous avons conclu qu'il y avait utilisation frauduleuse du numéro d'assurance sociale. Mais il y a eu des enquêtes liées à l'utilisation potentiellement frauduleuse d'un NAS.

Dans la plupart des cas — je dirais que pour les deux tiers —, il s'agissait aussi d'une enquête parallèle sur les prestations, et environ 1 400 portaient sur des problèmes possibles liés à des demandes de NAS.

Lorsque nous faisons enquête, il ne s'agit pas nécessairement de fraude; il se pourrait tout simplement qu'il y ait une indication dans le registre d'assurance sociale; à titre d'exemple, le détenteur d'un NAS est décédé, mais une autre personne se présente au bureau pour réactiver ce NAS ou obtenir une nouvelle carte d'assurance sociale. Avant de donner un numéro d'assurance sociale à une personne, nous la renvoyons à notre enquêteur interne pour qu'il la questionne davantage et qu'il obtienne d'autres pièces d'identité afin de confirmer si, oui ou non, le requérant faisant la demande de numéro d'assurance sociale n'est pas un imposteur.

• (1125)

L'hon. Laurie Hawn: S'agirait-il là d'une fraude délibérée ou accidentelle...? Est-ce tout simplement une erreur ou est-ce intentionnel?

M. Louis Beauséjour: Cela peut découler d'erreurs dans le serveur, ou quelquefois, il peut s'agir de véritables fraudes éventuelles. S'il s'agit d'une véritable fraude qui pourrait mener à d'autres types de fraude, nous aiguillons le dossier à la GRC afin qu'elle enquête et nous indique si c'est une véritable fraude ou pas.

L'hon. Laurie Hawn: À quelle fréquence envoyez-vous des dossiers à la GRC aux fins de poursuite?

M. Louis Beauséjour: Je n'ai pas cette information sous la main.

L'hon. Laurie Hawn: Est-ce fréquent ou plutôt rare? Je sais qu'il s'agit d'une évaluation subjective.

M. Louis Beauséjour: Je ne le sais pas.

L'hon. Laurie Hawn: Comment ces cas sont-ils débusqués? Est-ce tout simplement un employé qui estime que la situation est louche? Comment pérez-vous les fraudeurs?

M. Louis Beauséjour: Nous avons divers moyens. Parfois, ce sont des indices dévoilés par un dénonciateur. Comme je l'ai dit, ce peut être des personnes qui se présentent au bureau, sans avoir les bonnes pièces d'identité dont nous avons besoin. D'autres fois, elles n'ont pas de documents permanents, ou bien les documents qu'elles fournissent nous semblent louches.

Entre autres, les gens peuvent venir au bureau parce qu'on leur a transmis un T4 pour des prestations qu'ils n'ont jamais reçues. À ce moment-là, nous faisons enquête sur les prestations liées à ce document. Nous vérifions aussi si le NAS a été mal utilisé.

Voilà quelques exemples qui nous mettent la puce à l'oreille.

Un particulier peut aussi nous rencontrer directement pour nous signaler qu'il estime être victime d'un vol d'identité et qu'il souhaite obtenir un nouveau numéro d'assurance sociale. Dans ce cas-là, nous faisons enquête et renvoyons le dossier à la GRC pour déterminer s'il y a véritablement vol d'identité.

L'hon. Laurie Hawn: Avez-vous une idée du nombre de personnes qui se présentent à vous en disant qu'elles veulent un nouveau NAS parce qu'elles pensent être victimes de vol d'identité?

M. Louis Beauséjour: Je n'ai pas cette information précise, mais je pense que le chiffre maximum dont nous disposons... Comme je l'ai signalé, il n'y a qu'environ 1 400 personnes qui ont été recensées comme ayant des problèmes liés uniquement au NAS. Je suppose que cela signifie probablement un chiffre un peu plus élevé, mais je vais devoir faire des recherches pour voir si nous avons des chiffres précis là-dessus.

L'hon. Laurie Hawn: Vous avez donc renvoyé 1 400 dossiers à la GRC pour enquête supplémentaire. Ai-je bien compris?

M. Louis Beauséjour: Ce sont les dossiers que nous renvoyons à la GRC lorsque les gens nous disent être victimes de vol d'identité. Nous ne nous penchons pas sur les vols d'identité. Nous enquêtons sur toutes les questions touchant la délivrance d'un nouveau NAS ou d'une nouvelle carte d'assurance sociale. Nous faisons aussi enquête pour nous assurer que les prestations sont versées à la bonne personne.

L'hon. Laurie Hawn: Je comprends.

Vous ne permettez plus que cela se fasse par courrier, et je n'ai peut-être pas entendu ce renseignement, mais est-ce que quelqu'un peut présenter une demande de carte d'assurance sociale en ligne?

M. Louis Beauséjour: Non, on ne peut pas faire de demande en ligne. Les gens doivent se rendre au bureau pour obtenir une carte d'assurance sociale. Maintenant, les parents peuvent demander le numéro d'assurance sociale à la naissance lorsqu'ils enregistrent leur nouveau-né. C'est un nouveau programme mis en oeuvre dans toutes les provinces. C'est la seule façon.

L'hon. Laurie Hawn: Ma petite-fille est née dimanche, alors nous passons par ce processus actuellement.

C'est peut-être encore en dehors de votre champ de compétence, mais êtes-vous au courant des sanctions pour le vol d'identité ou

l'utilisation frauduleuse des cartes de NAS? Et si oui, pensez-vous qu'elles sont suffisantes? Ou devrait-on les examiner?

M. Louis Beauséjour: Je ne suis pas au courant... Je sais qu'il y a une sanction pour l'utilisation frauduleuse du NAS dans le cadre du programme. Je n'ai pas les détails avec moi. Je peux vous revenir là-dessus.

● (1130)

Le président: Monsieur Hawn, je suis désolé, mais cela met fin au temps que vous aviez. Merci beaucoup, et félicitations, grand-père.

Maintenant, pour les libéraux, nous avons... En fait, nous entendrons M. Andrews une fois qu'il sera de retour, car c'est lui qui siège au comité, mais nous accueillerons quand même l'honorable député de l'Île-du-Prince-Édouard, M. MacAulay.

L'hon. Lawrence MacAulay (Cardigan, Lib.): Merci beaucoup.

Je suis ici à titre de remplaçant, mais j'ai écouté votre exposé, qui m'a beaucoup plu, et je vous remercie d'être des nôtres.

Vous avez dit qu'on n'attribue plus le NAS sur une carte parce qu'elle était très pratique à transporter. J'en déduis qu'on s'inquiète beaucoup du fait que les gens ne protègent pas toujours assez leur identité, et c'est pourquoi on a changé cette mesure. J'aimerais que vous m'en disiez plus à ce sujet.

M. Louis Beauséjour: Les gens ne sont pas toujours conscients du risque qu'ils courent en transportant sur eux plusieurs pièces d'identité différentes. Nous faisons de notre mieux pour les sensibiliser à l'importance de la protection de ce genre de renseignements. Dans le cadre du Code de bonnes pratiques du NAS, sur le site Web, nous décrivons ce que les gens devraient et ne devraient pas faire avec leur numéro d'assurance sociale.

C'est l'une des raisons pour lesquelles nous avons décidé de ne plus produire de cartes. Les gens reçoivent toujours leur numéro d'assurance sociale lorsqu'ils se présentent au bureau, mais ils le reçoivent sur une feuille de papier. Voilà la seule chose que nous leur donnons.

L'hon. Lawrence MacAulay: Merci beaucoup. J'aimerais que vous me parliez des failles de sécurité comme celles de RHDCC. Les renseignements se trouvaient sur un petit appareil portatif. Pensez-vous que cela pose problème et que les renseignements personnels ne devraient pas être entreposés sur de tels appareils? J'aimerais que vous nous donniez votre opinion là-dessus.

M. Louis Beauséjour: Évidemment, nous croyons qu'ils ne devraient pas l'être, car nous avons changé nos pratiques. À l'heure actuelle, si ce genre de renseignements personnels doit être transféré sur ce type d'appareils, le tout sera chiffré pour en protéger le contenu. L'une des premières mesures que nous avons prises lorsque nous avons perdu le disque dur, c'est de nous assurer que ces appareils ne seraient plus utilisés et que notre système n'accepterait que les appareils chiffrés.

Nous avons également mis en place un système de prévention des pertes de données qui nous permet de contrôler ce qui est copié du système à un appareil. Nous surveillons également les appareils qui sont reliés aux ordinateurs du ministère, ou qui y sont insérés.

L'hon. Lawrence MacAulay: Les bris de sécurité sont liés au vol d'identité. Quel effet cela a-t-il sur les entreprises, et savez-vous quel pourcentage des failles sont liées à ce genre de vol? Il s'agit peut-être aussi de perte, mais j'imagine qu'il s'agit surtout de vol.

M. Louis Beauséjour: Je ne peux pas faire d'observations sur les conséquences générales du vol d'identité pour l'économie. Ce n'est pas quelque chose sur lequel on se penche.

L'hon. Lawrence MacAulay: J'aimerais que vous nous en disiez plus. Il semble que ce soit toujours une question de rattrapage, et c'est facile à comprendre. Mais il est parfois difficile de savoir qui fait ce rattrapage. Vous avez mis en place la formation d'accréditation pour les agents et le Code de bonnes pratiques du NAS. Pourriez-vous nous en dire un peu plus sur ce code?

M. Louis Beauséjour: Oui, le Code de bonnes pratiques du NAS nous permet de conseiller les employeurs, les intervenants et les personnes sur ce qu'ils devraient ou ne devraient pas faire pour protéger les renseignements personnels.

Voici un exemple pour les employeurs: nous recommandons qu'ils n'utilisent pas le numéro d'assurance sociale comme numéro d'identité de l'employé dans leur système, et nous recommandons également qu'ils n'incluent le numéro d'assurance sociale dans les lettres que si nécessaire, comme pour un TE. Mais pour les autres types de communication, nous recommandons qu'ils ne transmettent pas le numéro d'assurance sociale. C'est un des exemples inclus au code, afin de mieux les informer sur l'importance de la protection du numéro d'assurance sociale, en particulier.

• (1135)

L'hon. Lawrence MacAulay: Bien.

Le NAS est utilisé pour identifier les gens. S'il n'a pas été utilisé pendant cinq ans, vous avez dit qu'un indicateur est ajouté afin de... Est-ce pour enquêter sur ce qui s'est produit? Est-ce pour détecter la fraude fiscale ou ce genre de choses? J'aimerais le savoir.

M. Louis Beauséjour: Je ne peux pas parler de fraude fiscale. C'est l'ARC qui serait en meilleure position pour indiquer quelles sont les techniques utilisées pour la détecter. Nous ajoutons l'indicateur inactif lorsque les gens quittent le pays — la plupart du temps, c'est parce qu'ils ne sont plus au pays ou qu'ils sont dans une zone de guerre; bref, on ne sait plus où ils sont. Plus le temps passe, plus il y a un risque d'utilisation frauduleuse si une personne veut réactiver le NAS. C'est pourquoi nous utilisons ce que nous appelons l'indicateur inactif. C'est un indicateur au dossier d'assurance sociale qui indique que... Dans ce cas, les personnes qui veulent utiliser à nouveau leur numéro d'assurance sociale doivent venir au bureau pour le réactiver. Cela nous donne une garantie supplémentaire que c'est la bonne personne qui veut réactiver son NAS. C'est pour faire en sorte que la bonne personne reçoive les bonnes prestations.

M. Robert Frellich (directeur, Division des Services d'identité des entreprises, Service Canada, ministère de l'Emploi et du Développement social): L'indicateur inactif est l'un des éléments qui permettent aux agents d'examiner plus en détail le dossier d'assurance sociale, et si le numéro n'a pas été utilisé pendant une longue période, c'est l'un des facteurs supplémentaires dont on tient compte avant d'approuver la réactivation d'un NAS. S'il y a quelque chose qui cloche, s'il y a une personne qui, par exemple, ne correspond pas aux documents ou à la description de la situation, on renvoie le dossier au centre national d'identité à des fins d'enquête.

Le président: Merci, monsieur Frelons, et merci monsieur MacAulay. Malheureusement, c'est tout le temps que vous aviez.

Nous allons maintenant passer à Pat Davidson, qui présente les conservateurs. Pat, vous avez sept minutes.

Mme Patricia Davidson (Sarnia—Lambton, PCC): Merci beaucoup, monsieur le président.

Merci beaucoup, messieurs, d'être ici aujourd'hui dans le cadre de cette étude extrêmement importante que nous entamons.

J'avais deux questions à vous poser au sujet des observations que vous avez faites.

La première touche à la question de M. MacAulay sur le statut inactif de la carte d'assurance sociale. Vous dites que si elle a été inactive pendant cinq années consécutives ou plus, on peut y ajouter un indicateur inactif. Vous avez dit également qu'on l'utilise pour l'impôt et ce genre de choses. Par contre, vous avez ajouté qu'un enfant peut recevoir son NAS à la naissance. Alors, quelle est l'utilisation de ce NAS? Les enfants ne produisent pas de déclarations de revenus. Comment utiliseraient-ils leur NAS? Leur NAS deviendrait-il systématiquement inactif, et faudrait-il le réactiver?

M. Louis Beauséjour: Je devrai vous revenir sur les détails du processus. Mais la raison pour laquelle les parents aiment avoir le numéro d'assurance sociale à la naissance, c'est pour contribuer au régime d'épargne-études et obtenir les subventions qui y sont liées. Voilà, en gros, une des raisons.

Mme Patricia Davidson: Alors si un REEE est ouvert, la carte est utilisée.

M. Louis Beauséjour: Oui, c'est vu comme une utilisation du programme.

M. Robert Frellich: Dans le cadre de nos échanges de données de l'état civil avec les provinces et les territoires, lorsque l'enfant reçoit le certificat de naissance de la province, on indique au dossier d'assurance sociale que le NAS a été émis à la naissance lors de l'enregistrement de la naissance.

Mme Patricia Davidson: Bien. Merci.

L'un des problèmes auxquels la plupart des députés doivent faire face, ce sont les faux courriels envoyés à nos électeurs. Souvent, il s'agit de courriels qui imitent les agences gouvernementales comme Revenu Canada ou Service Canada.

Tout récemment, j'ai eu des échanges avec des électeurs au sujet de cas d'hameçonnage. Pourriez-vous nous dire si vos ministères essaient d'informer la population au sujet de ce genre de fraude, et comment vous le faites?

• (1140)

M. Louis Beauséjour: Depuis des années, nous indiquons sur notre site Internet que Service Canada ne rejoint pas ses clients de cette façon. Plus récemment, nous avons décidé d'aller plus loin. Nous l'avons mis encore plus en évidence sur la page d'accueil du site Web de Service Canada pour que les gens sachent qu'ils pourraient avoir affaire à de l'hameçonnage. Il y a un lien vers une page plus détaillée où l'on explique qu'ils ne devraient pas répondre à ce genre de courriels et où l'on donne des exemples de stratégies d'hameçonnage possibles.

Nous continuons de prendre l'initiative de mettre cela en évidence sur la page de Service Canada afin que les gens soient au courant de ce genre d'escroqueries.

Mme Patricia Davidson: Est-ce qu'une personne doit se rendre sur le site Web de Service Canada pour voir ces renseignements? Ne sont-ils pas disponibles ailleurs?

M. Robert Frelich: En fait, nous avons vu des tentatives d'hameçonnage dans le contexte du site Web de la banque d'emplois du gouvernement. Nous avons affiché des messages sur cette page pour indiquer, entre autres, que la banque d'emplois ne vous demandera pas de fournir des renseignements financiers, ni de payer un montant, et qu'il s'agit ici du seul site Web valide de la banque d'emplois.

Le Centre antifraude du Canada a un site Web qui présente les indices à repérer, comme les tentatives d'hameçonnage, et la façon de prévenir la fraude et le vol d'identité, entre autres.

Mme Patricia Davidson: J'imagine qu'on n'utilise plus beaucoup maintenant les lettres à la poste, mais y a-t-il en fait des avis qui sont envoyés de cette façon aux électeurs?

M. Louis Beauséjour: Je devrai vérifier. Je ne crois pas que nous insérions systématiquement un feuillet sur l'hameçonnage lorsque nous envoyons des renseignements par courrier, mais je vais quand même vérifier. Je ne crois pas que nous le fassions. En fait, comme je l'ai dit, Internet est maintenant devenu la voie préférée pour transmettre les renseignements.

Mme Patricia Davidson: Bien.

Nous savons tous qu'il est extrêmement important de protéger les renseignements personnels des Canadiens. Il est clair que le gouvernement doit protéger les renseignements personnels de ceux qui sont servis par les ministères gouvernementaux comme Service Canada, Revenu Canada, ou les autres.

La commissaire à la protection de la vie privée a dit clairement que toute atteinte importante à la protection des renseignements personnels devrait lui être signalée.

Pourriez-vous nous expliquer ce qui, d'après vous, constitue une atteinte importante et ce qui la distingue d'un incident qualifié de moins grave, qu'on n'aurait peut-être pas besoin de déclarer au Commissariat à la protection de la vie privée?

M. Louis Beauséjour: En fait, il ne s'agit pas de mon opinion, mais il y a une entente sur les trois caractéristiques d'une atteinte qu'il faut déclarer à la commissaire.

D'abord, les renseignements doivent être directement reliés à des renseignements personnels de nature sensible, comme des renseignements financiers ou médicaux, ou à un identifiant personnel comme le numéro d'assurance sociale. Ensuite, il doit y avoir un risque de vol ou de fraude d'identité. Enfin, l'incident peut nuire à la carrière, la réputation, la situation financière, la sécurité, la santé ou au bien-être de la personne.

Voilà les critères utilisés pour déterminer s'il est nécessaire de déclarer une atteinte à la commissaire à la protection de la vie privée.

• (1145)

Le président: Cela met fin à vos sept minutes. Merci beaucoup.

M. Andrews est arrivé en retard et a demandé la permission de poser une petite question. Le comité est-il d'accord pour permettre à M. Andrews de le faire?

Des voix: D'accord.

Le président: Allez-y, Scott, après quoi nous passerons au NPD.

M. Scott Andrews (Avalon, Lib.): Merci.

Je viens de passer en revue votre mémoire.

Est-ce qu'il y a des restrictions pour les autres organisations qui veulent utiliser le NAS d'une personne afin de l'identifier en tant que client ou autre? Un organisme gouvernemental externe peut utiliser le NAS d'une personne pour l'identifier comme client, ou à d'autres fins. Cela sort de la relation employeur-gouvernement. Il s'agit d'une organisation externe qui utilise le NAS. Y a-t-il des restrictions pour les entreprises qui voudraient faire cela?

M. Louis Beauséjour: Une organisation peut utiliser le NAS comme identifiant par l'intermédiaire, je pense, du Secrétariat du Conseil du Trésor, mais il y a des limites juridiques en ce qui concerne ceux qui peuvent demander cette information ou ceux à qui nous pouvons demander de fournir un NAS. Nous informons les clients sur ce qu'ils ne devraient pas faire: ne pas donner leur NAS à ceux qui le demandent, à moins qu'ils aient la capacité juridique de le faire et qu'ils proposent d'autres façons de confirmer votre identité. Les gens peuvent fournir des permis valides ou d'autres pièces d'identité. Mais ils ne devraient pas donner leur NAS, sauf si l'organisation qui le demande a le droit de le faire légalement.

Le président: Merci, monsieur Beauséjour.

Merci, Scott.

Nous passons maintenant aux néo-démocrates qui vont diviser leur temps de parole, et nous n'aurons que le temps d'entendre une intervention de cinq minutes du NPD, suivie d'une autre intervention de cinq minutes de la part des conservateurs. Puis, nous prendrons quelques instants pour faire venir l'autre groupe de témoins, car il y aura deux exposés de 10 minutes. Cela signifie que la deuxième partie de la séance sera écourtée.

Mathieu, vous vouliez débiter?

[Français]

M. Mathieu Ravignat: Pour commencer, j'aimerais présenter l'avis de motion suivant:

Que, conformément à l'alinéa 108(3)h)(iv), le Comité invite la commissaire à la protection de la vie privée du Canada à présenter les conclusions de l'Enquête sur la perte d'un disque dur à Emploi et Développement social Canada.

Merci, monsieur le président.

[Traduction]

Le président: Alors vous ne faites que présenter un avis de motion.

[Français]

M. Mathieu Ravignat: Oui.

Je vais maintenant céder la parole à mon collègue, M. Giguère.

M. Alain Giguère (Marc-Aurèle-Fortin, NPD): Bonjour, monsieur Beauséjour.

Dans votre document, vous indiquez que le ministère ne recommande pas l'utilisation de la carte d'assurance sociale. Or j'ai examiné ma carte d'assurance sociale et il est écrit ceci à l'endos: « Signez votre carte. Gardez-la sur vous ». Maintenant, vous dites que vous ne recommandez pas aux gens de la garder sur eux. Pourtant, quand vous émettez cette carte, vous leur demandez expressément de le faire. J'y vois une contradiction majeure.

M. Louis Beauséjour: Votre carte a probablement été émise il y a un certain nombre d'années, car les nouvelles cartes portent une mention à l'endos disant de ne pas la garder sur soi. Cela démontre simplement que, au fil des années, on s'est aperçu qu'il fallait changer nos pratiques concernant la protection du numéro d'assurance sociale dans la mesure où il y avait un risque de vol d'identité lorsque les gens la gardaient sur eux.

Je ne peux pas dire depuis combien de temps on a changé les cartes. Récemment, on a fêté le 50^e anniversaire du numéro d'assurance sociale. Cela fait 50 ans cette année que le numéro d'assurance sociale existe.

M. Alain Giguère: Ma question est tout à fait du même genre que celle de mon collègue.

J'aime bien vos envolées, mais nous procédons actuellement à une réforme supposément démocratique au nom de laquelle on interdit aux électeurs de se présenter avec leur fiche d'électeur, mais on leur demande de se présenter avec leur carte d'assurance sociale pour qu'ils puissent voter.

D'un côté, le ministre d'État responsable de la Réforme démocratique nous dit de ne plus utiliser la fiche d'électeur, mais d'utiliser plutôt la carte d'assurance sociale. De l'autre, vous venez de nous informer que cette carte n'existera plus. Il serait intéressant que les ministères se parlent de temps à autre.

On ne peut pas utiliser à des fins d'identification de l'électeur une carte qui n'existera plus bientôt. Il y a un problème à cet égard.

• (1150)

M. Louis Beauséjour: Puisque la carte n'existera plus, cela deviendra un enjeu. Nous allons devoir faire un suivi à ce sujet. Je ne sais pas ce qui s'est passé.

M. Alain Giguère: Vous dites qu'il existe toujours un danger. C'est manifestement le cas. Quand on perd son portefeuille, on perd sa carte d'assurance sociale et d'autres renseignements pertinents, particulièrement ceux qui sont inscrits sur le permis de conduire. Toutefois, il ne se vole pas 500 000 portefeuilles par année au Canada.

Quant à votre ministère, en une seule opération, il a perdu 500 000 renseignements personnels. L'ordre de grandeur n'est pas le même. À cet égard, le commissaire à l'information et à la protection de la vie privée affirmait que, pour l'ensemble des ministères fédéraux, seulement 4,4 % des pertes de renseignements lui sont signalées.

Ne pensez-vous pas que votre priorité devrait être de sécuriser davantage vos réseaux internes de transmission de données plutôt que de dire aux citoyens canadiens de se méfier des voleurs de portefeuille?

Je ne crois pas qu'il se vole 500 000 portefeuilles par année au Canada. La principale source de danger n'est pas que les citoyens perdent leur portefeuille, mais bien qu'ils se fassent voler leur identité. La carence de votre ministère est de ne pas toujours bien conserver et protéger les renseignements dont il est le dépositaire.

M. Louis Beauséjour: Comme je viens de le mentionner, la protection des renseignements personnels qui nous sont confiés est au coeur de nos préoccupations à l'échelle du ministère. Nous essayons constamment de nous améliorer.

À la suite des événements que vous avez mentionnés, nous avons mis en place différentes mesures de renforcement de la protection et nous sommes constamment à l'affût de nouvelles manières de réduire les risques associés à la perte de renseignements personnels.

[Traduction]

Le président: Merci, monsieur Beauséjour.

Merci, monsieur Giguère.

Malheureusement, vous n'avez plus de temps.

Ensuite, du côté des conservateurs, nous passons à Jacques Gourde.

Il s'agira de la dernière question.

[Français]

M. Jacques Gourde (Lotbinière—Chutes-de-la-Chaudière, PCC): Merci, monsieur le président.

Je remercie également M. Beauséjour pour les informations qu'il nous a données aujourd'hui.

Personnellement, j'aimais bien la carte d'assurance sociale. Elle me créait un lien avec le gouvernement du Canada. J'ai demandé ma carte à l'âge de 16 ans et je me rappelle que c'est avec fierté que je l'ai reçue. Pour moi, la carte constituait aussi un aide-mémoire.

Bientôt, le ministère va nous faire parvenir notre numéro d'assurance sociale sur une feuille de papier. Les gens, surtout les jeunes, seront portés à placer la lettre avec leurs affaires et à la perdre facilement.

Le ministère doit s'attendre à recevoir de nombreux appels pour recevoir à nouveau le numéro. Comment allez-vous faire pour offrir ce service à l'ensemble de la population canadienne?

M. Louis Beauséjour: Au moment de l'émission du numéro d'assurance sociale, nous demanderons au client de mémoriser rapidement son numéro et de garder la lettre que nous lui avons envoyée dans un endroit sécuritaire afin de pouvoir s'y référer au besoin.

Au cours des prochains mois, nous allons évaluer la situation afin de mesurer les incidences du retrait de la carte d'assurance sociale. Nous ne croyons pas que l'incidence sera très importante, mais nous allons faire un suivi très serré du nombre de personnes qui communiqueront régulièrement avec nous pour obtenir à nouveau leur numéro d'assurance sociale.

M. Jacques Gourde: Dans combien de temps cesserez-vous d'émettre la carte d'assurance sociale?

M. Louis Beauséjour: Nous avons cessé d'émettre des cartes d'assurance sociale lundi dernier. Nous ne connaissons pas encore l'incidence que cette mesure aura sur le réseau, mais nous ferons un suivi de la situation.

M. Jacques Gourde: Je peux prévoir que vous allez avoir d'énormes problèmes parce que, présentement, au Canada, les gens déménagent plus souvent qu'auparavant. Souvent, lors de déménagements, on perd des papiers. Les jeunes aussi déménagent beaucoup.

Je pense que vous avez créé un monstre sans le vouloir. Je ne veux pas vous décourager. On va avoir plus de travail dans les bureaux de députés parce que les gens vont nous appeler pour nous demander quoi faire pour obtenir un nouveau numéro d'assurance sociale. Je pense que vous allez devoir mettre en place une cellule d'urgence parce que, d'ici quelques mois, ça va commencer.

●(1155)

M. Louis Beauséjour: J'en prends note. Comme je l'ai dit, on va faire un suivi de l'impact que cela aura sur le réseau. J'imagine qu'à ce moment-là, s'il y a des mesures à prendre, on regardera quelles seront celles qui seront approuvées.

M. Jacques Gourde: Vous demandez aux gens de mémoriser leur numéro. À un certain âge, on a de la difficulté à se rappeler des numéros. Ce n'est pas tout le monde qui a de la facilité à mémoriser des numéros.

Je pense que ce que vous dites est un argument relativement faible pour expliquer cette décision.

M. Louis Beauséjour: Comme je l'ai dit, la personne va pouvoir se référer à son document qui sera à la maison. C'est clair que ce sera un document important qu'il faudra garder dans un endroit sécuritaire.

On fait la même recommandation, que ce soit pour la carte ou le document. On a toujours recommandé au cours des dernières années de ne pas transporter la carte d'assurance sociale sur soi. Alors, que ce soit la carte ou la lettre, c'est exactement la même chose: elle doit être préservée dans un endroit sécuritaire.

Les gens doivent s'assurer qu'ils peuvent la retrouver. C'est clair qu'il y a un risque, mais ce risque existe depuis plusieurs années. Cela fait plusieurs années qu'on recommande aux gens de ne pas transporter leur carte d'assurance sociale sur eux. On espère qu'ils suivraient cette recommandation parce que cela mettrait leur identité à risque.

M. Jacques Gourde: Avez-vous calculé le nombre de fois qu'un Canadien doit inscrire son numéro d'assurance sociale sur un formulaire au cours d'une année?

M. Louis Beauséjour: Non, je ne sais pas combien de fois il doit le faire. C'est clair qu'il y a un certain nombre de programmes pour lesquels on doit le faire. C'est sûr que chaque fois qu'une personne trouve un nouvel emploi et a un nouvel employeur, elle doit lui donner son numéro d'assurance sociale.

De plus, pour tous les programmes du gouvernement fédéral qui offrent des prestations, la personne doit aussi donner son numéro d'assurance sociale. Tout dépend où la personne en est dans son cycle de vie. Certains occupent le même emploi depuis plusieurs années et doivent rarement donner leur numéro d'assurance sociale alors que d'autres doivent le faire plus fréquemment.

M. Jacques Gourde: Merci.

[Traduction]

Le président: Merci, monsieur Gourde. Cela met fin au temps que vous aviez. C'est parfait.

Messieurs Beauséjour et Frelich, merci beaucoup d'être venus nous voir aujourd'hui. Ce fut très utile.

Nous allons maintenant suspendre brièvement la séance pour accueillir un nouveau groupe de témoins. Je propose aux membres du comité qu'ils profitent de l'occasion pour se servir à dîner. Nous allons reprendre dans environ cinq minutes.

●(1155)

_____ (Pause) _____

●(1200)

Le président: Nous allons maintenant demander aux témoins de faire leurs exposés.

Nous recevons des représentants de deux ministères: le ministère de la Citoyenneté et de l'Immigration et le ministère de l'Industrie. Les deux témoins aimeraient pouvoir faire un bref exposé préliminaire, de 5 à 10 minutes. Nous allons certainement leur donner cette occasion.

Les membres du comité doivent être conscients que nous avons besoin de 5 à 10 minutes à la fin de la séance pour donner au greffier des directives sur les témoins à venir. Alors le nombre de tours de questions pour ces témoins sera limité.

Cela dit, nous allons accueillir, du ministère de la Citoyenneté et de l'Immigration, M. Lu Fernandes, directeur général de la Direction générale de l'intégrité du Programme de passeport.

Monsieur Fernandes, je crois que vous ferez un exposé au nom de votre ministère. Veuillez débiter, monsieur.

M. Lu Fernandes (directeur général, Direction générale de l'intégrité du Programme de passeport, ministère de la Citoyenneté et de l'Immigration): Merci beaucoup.

Monsieur le président, mesdames et messieurs les membres du comité, je vous remercie de votre invitation, et c'est avec plaisir que nous contribuons à vos travaux visant à mieux comprendre le vol d'identité au Canada.

Je m'appelle Lu Fernandes. Je suis le directeur général de la Direction générale de l'intégrité du Programme de passeport à Citoyenneté et Immigration Canada. Je suis accompagné aujourd'hui par Peter Bulatovic, directeur à la Direction des enquêtes au sein de la Direction générale de l'intégrité du programme de passeport.

Plus de cinq millions de demandes sont traitées annuellement, et quelque 23 millions de documents de voyage canadiens valides sont en circulation. Notre passeport est vraiment l'un des symboles les plus distinctifs de la citoyenneté canadienne dans le monde entier. Et nous partageons la crainte que ces documents soient seulement délivrés aux citoyens canadiens qui y ont droit.

[Français]

À titre d'information, depuis le 2 juillet 2013, le ministre de la Citoyenneté et de l'Immigration assume l'entière responsabilité du Programme de passeport, y compris la délivrance, le refus de délivrer, la révocation, la retenue, la récupération et l'utilisation des passeports canadiens. Le ministre est également chargé de fournir des conseils aux missions qui délivrent des passeports à l'étranger et de superviser toutes les questions relatives aux documents de voyage canadiens.

À cette date, la prestation des services nationaux dans le cadre du Programme de passeport devient la responsabilité du ministre de l'Emploi et du Développement social, alors que le ministère des Affaires étrangères, du Commerce et du Développement continue d'offrir les services de passeport aux Canadiens à l'étranger.

[Traduction]

Ce transfert à CIC place la délivrance d'un passeport en fin de parcours dans le continuum des services fournis par un ministère qui facilite l'accès à ceux qui souhaitent visiter le Canada pour y étudier, y travailler, y immigrer et, éventuellement, demander la citoyenneté canadienne. Il confie également la prestation nationale de ces services à l'organisme de prestation de services du gouvernement, Service Canada.

- (1205)

[Français]

Alors que la modernisation du Programme de passeport se poursuit, ces changements permettent aussi de tirer profit des investissements réalisés dans la technologie actuelle, notamment le Système mondial de la gestion des cas de CIC et du vaste réseau de bureaux de Service Canada d'un océan à l'autre.

J'aimerais maintenant prendre quelques minutes pour parler des responsabilités directes du Programme de passeport.

[Traduction]

Le 1^{er} juillet 2013 marquait le lancement de notre passeport électronique et l'ajout d'une nouvelle option pour les Canadiens: la possibilité de choisir entre un passeport d'une durée de validité de 5 ou de 10 ans. Le nouveau passeport électronique respecte les normes internationales les plus récentes établies par l'Organisation de l'aviation civile internationale, que l'on considère comme la référence en matière de document de voyage.

La puce électronique intégrée dans le passeport ajoute un niveau de sécurité supplémentaire pour se prémunir contre le vol d'identité. La puce renferme les renseignements qui figurent à la page 2 du passeport, y compris la photo du titulaire, procurant ainsi au personnel de contrôle frontalier un outil supplémentaire pour valider l'identité du titulaire du passeport. En consultant l'information sur la puce et en la comparant aux renseignements indiqués à la page 2 du livret, un agent des services frontaliers peut s'assurer que l'information ou la photo n'a pas été modifiée.

La conception des pages de visa dans le passeport électronique offre un autre niveau de sécurité, ce qui rend le livret plus difficile à contrefaire. Les pages sont constituées de paires de vignettes uniques qui illustrent des thèmes, des lieux et des personnages marquants de l'histoire du Canada. Grâce aux différentes images sur chaque page et à divers éléments de sécurité visibles et invisibles, il est très difficile et extrêmement coûteux pour les faussaires de reproduire un livret ou de substituer une page.

[Français]

Le Programme de passeport s'engage à protéger la sécurité et l'intégrité des documents de voyage canadiens, ce qui est essentiel pour s'assurer qu'ils continuent à être acceptés à l'échelle internationale et faciliter les déplacements fréquents sans visa pour les Canadiens partout dans le monde.

Le Programme de passeport suit un protocole strict, qui favorise l'intégrité des documents eux-mêmes, pour valider l'identité et déterminer l'admissibilité à un passeport. Les personnes âgées de plus de 16 ans qui demandent un passeport pour la première fois doivent présenter un formulaire de demande accompagné de photos certifiées, d'une preuve de citoyenneté canadienne, de pièces d'identité à l'appui et de la déclaration du répondant.

[Traduction]

Les personnes qui possèdent déjà un passeport canadien peuvent utiliser le processus de renouvellement simplifié. Ce processus

repose sur un formulaire abrégé, et les requérants n'ont qu'à présenter leur passeport précédent et de nouvelles photos. La preuve de citoyenneté, les pièces d'identité à l'appui et la déclaration du répondant ne sont pas exigées, puisque ces renseignements se trouvent déjà au dossier dans le cadre du Programme de passeport.

Avant de délivrer un passeport, différents processus sont appliqués pour authentifier l'identité. Nous avons recours aux services d'agents bien formés et à des outils technologiques pour vérifier l'identité des requérants.

Au moment de présenter la demande, les renseignements personnels, les photos et les signatures sont comparés manuellement aux renseignements fournis dans les demandes de passeport antérieures, aux preuves documentaires de citoyenneté et aux pièces d'identité à l'appui.

Un logiciel de reconnaissance faciale est utilisé pour comparer les photos de chaque requérant par rapport à celles qui figurent dans la base de données de tous les titulaires de passeports pour faire échouer les tentatives de fraude d'identité.

D'autres vérifications automatisées comprennent la comparaison des renseignements personnels à ceux contenus dans la base de données centrale et sur la liste de surveillance du programme.

Si l'identité du requérant est mise en doute, d'autres vérifications peuvent être effectuées, notamment la vérification du répondant, des références et de la profession, la validation des documents d'identité de citoyenneté ou les requêtes adressées au Centre d'information de la police canadienne, le CIPC. En fait, nous communiquons quotidiennement par voie électronique avec Service correctionnel Canada afin d'obtenir des renseignements sur les délinquants sous responsabilité fédérale.

[Français]

Le Programme de passeport collabore étroitement avec d'autres ministères et des partenaires du milieu de l'application de la loi et du renseignement en ce qui concerne le refus de services de passeport et la révocation de passeports canadiens, s'il y a lieu.

Par exemple, les documents de voyage sont annulés lorsqu'une personne est incarcérée ou qu'elle fait l'objet d'autres restrictions relatives aux déplacements. Une personne qui est accusée ou déclarée coupable d'une infraction grave, ou qui doit des sommes de pension alimentaire, peut voir son passeport révoqué et se voir refuser les services de passeport.

- (1210)

[Traduction]

Le Programme de passeport a également la capacité, au sein de la Direction générale de l'intégrité du Programme de passeport, de mener des enquêtes administratives pour déterminer si une personne est admissible à un passeport ou si elle pourra avoir recours aux services de passeport dans l'avenir.

Les personnes qui se sont vu refuser un passeport, ou dont le passeport a été révoqué, peuvent contester les décisions prises par le programme dans le cadre d'un contrôle judiciaire devant la Cour fédérale du Canada.

Le Programme de passeport revoit continuellement ses politiques et procédures pour s'assurer de répondre aux normes changeantes et aux exigences en matière d'intégrité. Nous sommes résolus à tirer parti de la technologie et à travailler avec d'autres ministères, les bureaux de l'état civil provinciaux, les partenaires internationaux et les organismes d'application de la loi pour contrer les attaques à l'endroit du Programme de passeport et limiter les risques de vol et de fraude d'identité.

Évidemment, les Canadiens doivent contribuer à se prémunir contre le vol d'identité en gardant en lieu sûr leurs titres de voyage et autres documents importants et en évitant toute divulgation inutile de renseignements personnels.

[Français]

J'espère que, grâce à cette intervention, vous avez maintenant une bonne idée des activités du Programme de passeport en matière d'authentification de l'identité et de prévention de la fraude.

C'est avec plaisir que nous allons maintenant répondre à vos questions.

Je vous remercie.

[Traduction]

Le président: Merci beaucoup, monsieur Fernandes.

Avant de poser les questions, nous allons entendre l'exposé de M. Michael Jenkin, directeur général du Bureau de la consommation du ministère de l'Industrie.

Monsieur Jenkin.

M. Michael Jenkin (directeur général, Bureau de la consommation, ministère de l'Industrie): Merci, monsieur le président.

Merci de m'avoir invité à m'entretenir avec vous aujourd'hui au sujet du vol d'identité.

Comme vous l'avez mentionné, je suis le directeur général du Bureau de la consommation, qui fait partie du Secteur de la politique stratégique d'Industrie Canada.

[Français]

Je voudrais parler d'un certain nombre d'activités et d'initiatives que le ministère a entreprises dans le but de protéger les consommateurs en ce qui a trait au vol d'identité.

[Traduction]

J'amorcerai cet exposé par la Loi sur la protection des renseignements personnels et les documents électroniques, puis je décrirai comment cette loi aide à protéger les Canadiens contre le vol d'identité. Ensuite, j'aborderai des éléments particuliers de la Loi canadienne anti-pourriel, dont l'application relève d'un certain nombre d'acteurs fédéraux. Pour terminer, je mentionnerai certaines initiatives d'information auxquelles mon bureau a participé, dont des initiatives de sensibilisation du public concernant la mise en oeuvre de la Loi canadienne anti-pourriel.

Je commence donc par la Loi sur la protection des renseignements personnels et les documents électroniques, ou LPRPDE. Cette loi établit les règles en ce qui concerne la collecte, l'utilisation et la divulgation de renseignements personnels par des organisations du secteur privé, comme les banques ou les entreprises de téléphonie, dans le cadre de leurs activités commerciales. Bien que le ministre de l'Industrie détienne la responsabilité de la loi, son application et son administration incombent au Commissariat à la protection de la vie privée du Canada, qui agit de façon autonome. Ainsi, je m'en remets au commissariat pour toute question concernant l'application de la loi. Cela étant dit, je prendrai quelques minutes pour présenter un

aperçu de la loi et expliquer comment ces exigences aident à s'attaquer au vol d'identité.

[Français]

Les règles de la loi se fondent sur 10 principes reconnus à l'échelle internationale qui indiquent aux organisations les meilleures façons de gérer les renseignements personnels de leurs clients. Plusieurs de ces règles aident à protéger les consommateurs contre des menaces comme le vol d'identité.

[Traduction]

Par exemple, la loi requiert que les organisations recueillent seulement les renseignements dont elles ont besoin et qu'elles les conservent uniquement le temps nécessaire afin d'éviter de maintenir des bases de données contenant des renseignements personnels qui ne leur sont d'aucune utilité et qui seraient vulnérables à la perte ou au vol.

La loi exige en outre que les organisations mettent en place des mesures de sécurité raisonnables pour assurer la protection des renseignements personnels qu'elles détiennent contre l'accès non autorisé, la perte ou le vol. Ces mesures de sécurité, parmi lesquelles figure le recours à des mots de passe ou au cryptage des données des consommateurs, aident à prévenir la perte de renseignements personnels qui sont utilisés pour usurper l'identité d'individus.

En réponse au premier examen parlementaire de la LPRPDE, le gouvernement a pris l'engagement de modifier la loi afin d'y ajouter l'obligation pour les organisations d'aviser les individus lorsque leurs renseignements personnels ont fait l'objet d'une atteinte potentiellement préjudiciable. Grâce à ces modifications, les consommateurs seront assurés d'être prévenus en cas de perte ou de vol de leurs renseignements personnels, et ils recevront également les informations dont ils auront besoin pour se protéger contre le vol d'identité, la fraude, des pertes financières ou d'autres formes de préjudice. Le gouvernement demeure résolu à apporter ces modifications, de même que d'autres changements recommandés par le Parlement à la suite de son premier examen.

Je vous adresserai maintenant quelques mots au sujet de la Loi canadienne anti-pourriel.

● (1215)

[Français]

Cette loi interdit l'envoi non sollicité de messages électroniques à caractère commercial. Elle proscriit également l'installation de logiciels dans l'ordinateur d'un tiers sans consentement. Ensemble, ces deux interdictions constituent des mesures à l'égard des pourriels indésirables.

[Traduction]

La loi a notamment pour but de donner suite aux principales préoccupations suivantes: les « messages hameçons », qui sont conçus pour attirer les destinataires vers des sites Web truqués et les inciter à révéler des renseignements personnels comme des noms d'utilisateur, des mots de passe et des renseignements sur des comptes; les logiciels malveillants, qui sont installés dans l'ordinateur, le téléphone intelligent ou tout autre appareil numérique d'une personne à son insu et sans son consentement — ces logiciels espions et ces virus peuvent secrètement recueillir des renseignements personnels qui seront ensuite utilisés à des fins de vol d'identité; et enfin, le détournement du trafic, qui consiste à réacheminer secrètement les recherches en ligne d'une personne vers une destination frauduleuse où les attaquants pourront recueillir des renseignements personnels en vue de procéder à des vols d'identité.

La majeure partie de la Loi canadienne anti-pourriel entrera en vigueur le 1^{er} juillet 2014. À compter de cette date, la loi contribuera à protéger les Canadiens, tout en veillant à ce que les entreprises demeurent concurrentielles sur le marché mondial. Le 15 janvier 2015 marquera l'entrée en vigueur des articles de la loi portant sur l'installation non sollicitée de programmes informatiques ou de logiciels. Puis, les dispositions relatives au droit privé d'action entreront en vigueur le 1^{er} juillet 2017. Le Conseil de la radiodiffusion et des télécommunications canadiennes, ou CRTC, le Bureau de la concurrence et le Commissariat à la protection de la vie privée du Canada, ou CPVPC, sont chargés de l'application de la Loi canadienne anti-pourriel.

Le CRTC appliquera la loi en ce qui concerne les violations liées à l'envoi de messages électroniques commerciaux, la modification des données de transmission et l'installation de programmes informatiques sans consentement.

Le Bureau de la concurrence fera enquête et prendra des mesures contre les représentations fausses et trompeuses ainsi que les pratiques commerciales trompeuses.

Le CPVPC, pour sa part, enquêtera sur la collecte de renseignements personnels par le truchement d'accès illégaux à des réseaux informatiques et sur le prélèvement d'adresses électroniques.

[Français]

J'aimerais souligner que l'approche du gouvernement vise principalement à prévenir les problèmes avant qu'ils ne surgissent, et l'une des meilleures façons de le faire est de veiller à ce que les Canadiens comprennent comment se protéger eux-mêmes. Dans cette optique, le gouvernement a créé un site Web appelé www.combattrepourriel.gc.ca.

[Traduction]

En anglais, c'est www.fightspam.gc.ca.

Ce site Web comprend des renseignements sur la loi elle-même et offre un certain nombre de sources d'information aux Canadiens. Il abrite également le Centre de notification des pourriels, où les Canadiens peuvent transmettre des renseignements sur des messages électroniques à caractère commercial expédiés sans consentement, ainsi que sur des messages électroniques commerciaux à contenu faux et trompeur.

[Français]

J'ajouterai ici qu'une campagne en ligne a été amorcée pour informer les Canadiens de la date d'entrée en vigueur du 1^{er} juillet et les inviter à visiter le site Web www.combattrepourriel.gc.ca. Vous trouverez dans vos trousseaux une reproduction de la page d'accueil de ce site Web, de même qu'une représentation de la « Boîte à outils mobile », qui est l'un des produits d'information destinés aux consommateurs.

[Traduction]

Ma propre direction générale, le Bureau de la consommation, a participé à la préparation des communications relatives à la Loi canadienne anti-pourriel. Vous remarquerez que l'on a inséré une série de résumés infographiques dans les trousseaux qui vous ont été remis. Le premier, *Le pourriel vous inquiète? 5 choses à surveiller*, est destiné aux consommateurs pour leur offrir les renseignements de base dont ils ont besoin afin d'éviter d'être victimes de fraudeurs. Il révèle, à cet effet, un certain nombre de techniques très courantes utilisées par les polluposteurs pour obtenir les renseignements personnels de consommateurs. Le résumé infographique a été imprimé et distribué à un nombre considérable de parties intéressées,

parmi lesquelles on compte d'autres ministères fédéraux, des gouvernements provinciaux et des organismes communautaires.

Les trois autres résumés infographiques, *La Loi canadienne anti-pourriel s'applique-t-elle?*, *4 conseils pour communiquer électroniquement avec vos clients* et *3 éléments à considérer lors de l'envoi de messages*, ont été créés pour aider les PME à connaître les exigences fondamentales de la loi et, ainsi, éviter d'être confondues avec des polluposteurs. Ces trois résumés infographiques, plus celui que je viens d'évoquer, *Le pourriel vous inquiète?*, ont été publiés sur le site www.combattrepourriel.gc.ca et sont partagés au moyen du compte Twitter d'Industrie Canada.

● (1220)

[Français]

Enfin, vous trouverez de plus un document parmi ceux qui vous ont été remis. Celui-ci est intitulé « *Vol d'identité: une liste de vérification* »,

[Traduction]

En anglais, cela s'intitule *Identity Theft: A Checklist*.

[Français]

La liste a été élaborée en collaboration avec des responsables des gouvernements provinciaux et territoriaux et a été distribuée à grande échelle au cours des dernières années.

[Traduction]

Pour conclure, j'aimerais vous rappeler que le gouvernement a pris un certain nombre de mesures législatives destinées à protéger les Canadiens contre le vol d'identité. Parallèlement, la sensibilisation et l'éducation constituent une part importante de la solution à ce casse-tête; il s'agit de veiller à ce que les Canadiens disposent des renseignements nécessaires pour bien se protéger.

Merci, monsieur le président.

Le président: Merci, monsieur Jenkin. Votre exposé a été très utile.

Vu le manque de temps, nous allons passer à la première série de questions, à raison de sept minutes par personne: l'opposition officielle, puis les conservateurs, les libéraux et, de nouveau, les conservateurs. Après quoi, nous concluons. Nous devons en effet siéger à huis clos pour la planification d'affaires futures du comité.

Commençons donc, sans tarder, par M. Ravignat, qui dispose de sept minutes.

[Français]

M. Mathieu Ravignat: Merci, monsieur le président.

Je remercie les témoins d'être parmi nous aujourd'hui. C'est très gentil de leur part. Le fait d'avoir l'occasion de les entendre est toujours important pour les Canadiens et Canadiennes.

Ma première question s'adresse aux représentants du ministère de la Citoyenneté et de l'Immigration.

En réponse à une question au *Feuilleton* de mon collègue, M. Charlie Angus, vous avez indiqué que 174 atteintes aux données avaient affecté 246 Canadiens entre 2002 et 2012. Nous n'avons pas eu davantage de détails à ce sujet. Je me demandais si vous pouviez nous en dire davantage sur la nature de ces atteintes aux données.

M. Lu Fernandes: Je vous remercie de la question.

[Traduction]

En tant que responsable de la Direction générale de l'intégrité du Programme de passeport, je ne suis pas en mesure de répondre à la question que vous avez soulevée. Je ne sais pas si elle touche les passeports ou Citoyenneté et Immigration Canada.

[Français]

M. Mathieu Ravignat: D'accord.

À la suite d'une réponse à une question au *Feuilleton*, on nous a indiqué qu'il était impossible d'obtenir le nombre d'atteintes aux données au sein de votre ministère.

Selon vous, y a-t-il une raison spécifique qui explique ce manque d'information à ce sujet? Y a-t-il des lacunes dans la façon dont votre ministère s'assure de connaître les cas d'atteinte aux données. Pourriez-vous nous donner des détails à ce sujet? Par exemple, y a-t-il un système qui gère les cas d'atteinte aux données?

M. Lu Fernandes: Sauf le respect que je vous dois, je ne peux pas davantage répondre à ces questions qui touchent directement la perte de données.

[Traduction]

Je peux parler, en connaissance de cause, du Programme de passeport et de son intégrité.

M. Mathieu Ravignat: Parlons donc de l'intégrité des passeports. Y a-t-il un système en place pour gérer la perte de données de nature délicate?

M. Lu Fernandes: En cas de perte de données, ce sont les procédures et politiques habituelles qui s'appliqueraient: informer le Commissariat à la protection de la vie privée ou l'individu, selon la situation.

Comme je l'ai déjà expliqué, je suis chargé de l'intégrité du Programme de passeport lui-même, ainsi que de la sécurité du document, de sa délivrance et de l'examen de l'admissibilité.

• (1225)

M. Mathieu Ravignat: Ma prochaine question s'adresse à M. Jenkin.

Le travail que vous avez effectué sur le pourriel est intéressant. À ma connaissance, c'est l'un des rares exemples de travail accompli par le gouvernement pour renouveler son régime de protection des données personnelles. La loi n'a pas fait l'objet d'un examen depuis la création de Facebook et de Twitter. Il me semble que vous auriez des contributions intéressantes à apporter à la modernisation de la loi sur la protection des renseignements personnels et du cadre en vigueur.

Pour que les règles protégeant la vie privée des Canadiens à l'ère numérique soient plus robustes, quelles mesures envisageriez-vous?

M. Michael Jenkin: Sauf le respect que je vous dois, le Parlement a déjà effectué un examen de la loi, au terme duquel il a exprimé ses opinions, et le gouvernement y répondra sous peu. Je pense qu'il faut mener à bien ce processus de réforme, avant de se pencher sur de nouvelles menaces, de nouveaux problèmes ou de nouvelles questions ayant trait au vol d'identité.

Les choses évoluent très rapidement dans ce domaine, et il est parfois difficile de soutenir le rythme, étant donné l'évolution carrément... C'est d'ailleurs le cas pour les questions de fraude en général: les escrocs innovent sans arrêt, pour trouver de nouvelles façons de compromettre l'identité d'un particulier et de l'utiliser à mauvais escient.

Selon moi, la priorité pour l'instant est de mener à bien cette phase du travail, avant de s'attaquer aux problèmes futurs que le Parlement et le gouvernement jugeront tous deux importants.

Comme vous, nul doute, je pourrais énumérer une série de problèmes éventuels qui se dressent à l'horizon. Le hic, c'est qu'il faut aussi, dans ce domaine, laisser passer un certain temps avant de voir quelles sont les répercussions et de déterminer quels problèmes structurels à plus long terme il convient de régler dans cet environnement très innovateur et en évolution constante.

Bref, comme je l'ai dit, la priorité essentielle à l'heure actuelle est, selon moi, de mettre en oeuvre la réforme de la loi prévue par le gouvernement, afin de donner aux Canadiens plus de possibilités de se protéger dans le contexte actuel.

Le président: Votre temps est quasiment écoulé: il reste environ 10 secondes. Mais j'aimerais peut-être apporter une précision à la réponse de M. Jenkins.

La LPRDE doit faire l'objet d'un examen. Il aurait dû être effectué il y a deux ans environ. On a examiné la loi une fois, il y a environ sept ans, à la suite de quoi le gouvernement a déposé le projet de loi C-28, qui est mort au *Feuilleton*, puis le projet de loi C-12, qui a connu le même sort. Par conséquent, s'il y a eu des modalités adoptées par le gouvernement, aucune n'a été mise en oeuvre; la loi n'a jamais été modifiée.

Je ne veux pas que M. Ravignat pense que l'examen se soit conclu par des modifications à la loi. Ce n'est pas le cas.

Est-ce bien cela, ou vouliez-vous dire autre chose?

M. Michael Jenkin: Non, je voulais simplement dire que le gouvernement s'était engagé à examiner la loi en temps voulu et que la date était encore à déterminer. Mais le gouvernement s'est bien engagé à la modifier.

Le président: Et notre comité a d'ailleurs écrit au ministre pour demander que l'examen ait lieu.

Maintenant, nous passons à M. Zimmer, pour les conservateurs.

M. Bob Zimmer (Prince George—Peace River, PCC): Merci à nos témoins de leur comparution aujourd'hui.

Ma première question s'adresse à M. Fernandes.

J'aimerais savoir où se situe le Programme de passeport du Canada par rapport à celui des autres pays dans le monde. Sommes-nous les meilleurs? Sommes-nous les pires? Où nous classons-nous en matière de sécurité, soit la question dont nous sommes saisis aujourd'hui, par rapport au reste du monde?

• (1230)

M. Lu Fernandes: Merci.

Je suis très heureux de pouvoir dire que, relativement au document lui-même, nous en sommes à peu près au même niveau que les cinq nations que nous appelons des partenaires: les États-Unis, le Royaume-Uni, la Nouvelle-Zélande et l'Australie. Nous avons un document très sûr, par rapport à ce qu'il y a d'autre dans le monde, comme en témoignent les bons résultats sur le plan de sa sécurité proprement dite. Le passeport permet aux Canadiens d'avoir accès à quelque 140 pays, sans avoir besoin de visa.

C'est grâce au document, mais aussi au processus de vérification de l'admissibilité avant l'octroi d'un passeport canadien, et grâce aussi aux mesures de sécurité tant pour cet examen que pour l'identification du particulier. Le fait que tant de pays de par le monde soient accessibles aux Canadiens sans visa atteste de la qualité du document.

M. Bob Zimmer: Le ministère délivre un nouveau passeport électronique depuis quelques mois, sauf erreur de ma part. Pouvez-vous expliquer la différence entre ce nouveau passeport électronique, avec ses différents points ou avantages en matière de sécurité, et ce que nous avions auparavant?

M. Lu Fernandes: Oui, certainement, j'en serais heureux.

Le passeport électronique présente un niveau de sécurité accru et amélioré dans le livret lui-même, qui comporte une puce intégrée au dos de la couverture. La puce renferme les renseignements qui figurent à la page 2 du passeport, y compris la photo du titulaire.

On y trouve donc des données biographiques ainsi que la photo. Il s'agit d'une mesure de sécurité supplémentaire: ainsi, les agents frontaliers peuvent accéder à la puce, jeter un coup d'oeil aux renseignements et s'assurer qu'ils correspondent exactement à ce qu'on est censé voir sur la deuxième page du livret. C'est une sécurité accrue parce qu'ils ont ainsi un troisième point de référence: l'individu debout devant eux, la photo et la photo que comporte la puce. C'est là l'utilité de la puce électronique.

Quant au livret lui-même, si votre passeport est de l'ancien modèle, il comporte sur les pages de visa une série de feuilles d'érable en séquence d'une page à l'autre. Le livret du nouveau passeport électronique comporte, quant à lui, des vignettes sur chaque double page.

Avec votre permission, laissez-moi vous montrer, avec le pointeur, les éléments ultra-violet sur les pages elles-mêmes. Chaque page comporte des caractéristiques de sécurité visibles et invisibles intégrées qui fournissent d'autres paliers de sécurité, absents de l'ancien livret.

M. Bob Zimmer: J'en viens à ma dernière question — ou du moins, la dernière ayant trait aux passeports, car j'aurai d'autres questions pour Michael dans une minute. Quand on perd une carte de crédit ou qu'on se la fait voler ou peu importe, on commence par téléphoner à la banque pour le signaler, après quoi la banque émet une nouvelle carte, avec un nouveau numéro. Si on égare son passeport ou si on se le fait voler, y a-t-il des mesures de sécurité similaires qui permettent de protéger son identité et de se mettre à l'abri d'abus?

M. Lu Fernandes: Le processus de remplacement d'un passeport perdu — ou volé, dans bien des cas — est très différent du processus pour les cartes de crédit. Chaque année, on nous avise du vol ou de la perte de 66 000 passeports. Les Canadiens, tant au pays qu'à l'étranger, signalent de tels incidents. Souvent, ce sont des gens qui ont simplement oublié où ils ont mis leur passeport ou qui ont oublié dans quel carton ils ont bien pu le mettre lors d'un déménagement, et qui le déclarent perdu.

Quand la Direction de l'intégrité du Programme de passeport en prend connaissance, nous annulons automatiquement et immédiatement le livret. Dans les 24 heures qui suivent, nous avisons en outre nos partenaires que le livret a été déclaré perdu ou volé et qu'il a été annulé dans notre système.

Ce sont des renseignements que nous transmettons quotidiennement à l'ASFC. Nous prévenons également le Centre d'information de la police canadienne, le CIPC, que gère la GRC, afin que les

forces de police aient accès à cette information. Elle est mise à jour quotidiennement. Elle est ensuite transmise par le CIPC à Interpol, grâce à un lien entre la GRC et Interpol. C'est donc une information qui est transmise partout dans le monde dans la base de données d'Interpol.

Tout se fait sur le coup, en l'espace d'une journée. Le résultat? Si un particulier nous appelle pour nous dire qu'il ne trouve plus son passeport, qu'il doit l'avoir perdu, mais nous rappelle pour nous signaler qu'en fin de compte, il l'a retrouvé, nous l'informons clairement qu'il ne peut pas utiliser le livret. En effet, nous pourrions peut-être changer le statut du livret comme étant entre les mains de son détenteur, mais nous avons déjà informé tous nos partenaires que le livret a été annulé.

Le particulier ne peut donc pas utiliser le livret; il risquerait, ce faisant, d'être arrêté à la frontière. Il doit revenir nous voir et procéder à une nouvelle demande de passeport.

Merci.

●(1235)

M. Bob Zimmer: Est-ce qu'il me reste du temps, monsieur le président?

Le président: Non, je regrette, monsieur Zimmer, votre temps est écoulé. Merci.

Nous passons maintenant à M. Scott Andrews, qui représente les libéraux.

M. Scott Andrews: Merci.

Je reviendrai peut-être à la question, s'il me reste du temps, mais je vais commencer par autre chose.

Avez-vous des chiffres sur le nombre de personnes qui usurent une identité pour faire une demande de passeport? Combien de ces fraudeurs démasquez-vous?

M. Lu Fernandes: L'an dernier, nous avons refusé ou révoqué environ 1 370 demandes de passeport. Un millier de ces refus ou révocations avaient lieu pour cause de criminalité, c'est-à-dire qu'il s'agissait d'individus incarcérés faisant une demande de passeport à partir de leur lieu d'incarcération — une prison ou un pénitencier — ou encore d'individus frappés de restrictions en matière de déplacement, à la suite d'une incarcération. La très grosse majorité des cas que je viens de mentionner sont le fait de ce groupe, de cette population: 1 000 sur 1 370 cas.

Sur le chiffre total, on compte 70 individus à qui on a refusé un nouveau passeport ou retiré un passeport existant expressément à cause d'une usurpation d'identité.

M. Scott Andrews: D'accord. Que s'est-il passé pour ces 70 personnes? Les avez-vous signalées à la GRC? Quel est le processus, dans ces cas? Quelle est la raison la plus courante? Quels documents ou autres moyens ces gens utilisent-ils pour essayer de voler une identité? Ils vous donnent des documents pour prouver qui ils sont.

Vous comprenez mes deux questions?

M. Peter Bulatovic (directeur, Direction des enquêtes, direction générale de l'intégrité du Programme de passeport, ministère de la Citoyenneté et de l'Immigration): Oui.

Dans bien des cas, les personnes faisant la demande ont volé les documents de quelqu'un: carte de citoyenneté, certificat de naissance ou carte d'assurance-maladie. Ce sont des documents volés que la personne utilise pour faire une demande de passeport.

M. Scott Andrews: Comment les choses se déroulent-elles dans ces 70 cas, lorsque vous découvrez la supercherie?

M. Peter Bulatovic: Dans pareils cas, nous mettons un terme au processus de demande et nous lançons une enquête sur la personne. Nous l'avisons qu'elle fait l'objet d'une enquête et nous lui envoyons une lettre pour l'informer que nous ne pouvons pas donner suite à sa demande de passeport.

Souvent, s'il y a eu vol d'identité, nous n'entendons plus parler de la personne, si bien que, manifestement, l'enquête s'arrête là.

M. Scott Andrews: Est-ce qu'on signale à ces personnes que les pièces d'identité qu'elles essaient de faire admettre ont été volées?

M. Peter Bulatovic: Non, nous ne les en informons pas, parce que nous ne savons pas comment les documents ont été volés au juste. Nous ne connaissons pas la personne qui est en possession des documents. Nous ne savons pas si ces documents sont peut-être liés à un ami de la personne dont l'identité a été volée. Pour nous, c'est une zone vraiment grise.

• (1240)

M. Scott Andrews: Est-ce que vous rapportez l'incident à la GRC pour l'informer qu'une personne a essayé d'usurper l'identité d'une autre?

M. Peter Bulatovic: Oui.

M. Scott Andrews: Savez-vous ce que fait la GRC, une fois qu'elle est avisée?

M. Peter Bulatovic: C'est à la GRC qu'il faudrait poser la question. Il s'agit de savoir si la GRC a les ressources voulues pour enquêter sur chaque cas de vol d'identité.

M. Scott Andrews: Alors, au bout du compte, vous vous apercevez qu'il y a un problème, dans le cas de ces 70 personnes; vous en informez la GRC, et c'est tout.

M. Lu Fernandes: En fait, il y a aussi, pour plusieurs de ces cas, une enquête administrative au sein de la direction. Nous pouvons mener à bien les enquêtes nous-mêmes. Ce sont seulement les cas les plus graves de fraude ou de vol d'identité que nous signalons à la GRC.

M. Scott Andrews: À quelle fréquence vous arrive-t-il de révoquer un passeport déjà délivré, lorsque vous vous rendez compte que le détenteur a utilisé une identité qui n'était pas la sienne?

M. Peter Bulatovic: Eh bien, c'est ce qui se passe dans les 70 cas que le directeur général, Lu Fernandes, a mentionnés.

M. Lu Fernandes: En effet, c'est ce qui se passe dans les 70 cas que nous avons repérés.

M. Scott Andrews: D'accord. Mais combien de demandeurs obtiennent-ils effectivement un passeport, par opposition à ceux que vous arrêtez net?

M. Lu Fernandes: Je regrette, mais je n'ai pas la ventilation du chiffre.

M. Scott Andrews: Entendu. Vous dites que, généralement, le demandeur présente à Passeport Canada des documents qui ont été volés. Arrive-t-il qu'on présente des documents falsifiés pour obtenir un passeport?

M. Peter Bulatovic: Oui. On le découvre dans le cadre de nos enquêtes.

M. Scott Andrews: Cela arrive-t-il couramment?

M. Peter Bulatovic: La falsification de documents, on voit ça assez souvent.

M. Scott Andrews: Comment se protéger contre cette pratique? Pourrions-nous faire quoi que ce soit pour empêcher cela?

M. Peter Bulatovic: Pour nous, l'un des outils d'enquête les plus utiles est la reconnaissance faciale. Dès le moment où une personne présente une demande de passeport, nous effectuons une recherche pour apparier leur photo à celles qui figurent dans notre base de données. Disons que c'est sans doute la première ligne de défense pour lutter contre la fraude, dans ce domaine. Souvent, ainsi, la personne fait une demande en utilisant une identité que nous connaissons déjà. Nous savons alors qu'elle essaie d'utiliser un passeport en utilisant une identité valide que nous connaissons déjà.

Dans d'autres cas, notamment pour des gens qui présentent une demande pour la première fois, nous examinons la documentation de près et si quelque chose nous met la puce à l'oreille... Si, par exemple, une personne a eu maille à partir avec la police, son nom pourrait figurer dans la liste de surveillance du réseau; quand il y a appariement, nous nous penchons sur le cas. En l'occurrence, au lieu de traiter directement la demande de passeport, nous la transmettons à la division d'enquête pour qu'elle y regarde de plus près.

Le président: Vous avez 30 secondes, Scott.

M. Scott Andrews: Vous avez parlé d'environ 1 370 cas, dont 1 000 pour raison de criminalité et 70 pour l'autre raison. Qu'en est-il des 300 qui restent? Avez-vous une ventilation quelconque?

M. Lu Fernandes: Oui. Dans près de 225 cas, il s'agissait de fraude à l'admissibilité ou d'usage abusif d'un passeport. Permettre à quelqu'un d'utiliser votre passeport, par exemple, tomberait dans cette catégorie. Dans 36 autres cas, il s'agissait de problèmes de citoyenneté: un individu qui n'était pas, en fait, citoyen canadien.

M. Scott Andrews: Merci.

Le président: Tout le monde a fini.

Merci, Scott.

Enfin, pour conclure, nous passons à Tilly O'Neill Gordon, qui dispose de sept minutes.

Mme Tilly O'Neill Gordon (Miramichi, PCC): Merci, monsieur le président.

Je voudrais remercier tous nos témoins d'avoir bien voulu nous consacrer leur temps aujourd'hui.

C'est la première fois que je participe au comité et je suis curieuse de voir ce que notre étude nous permettra de cerner. Votre exposé d'aujourd'hui nous a, en tout cas, donné beaucoup d'information. C'est de l'information à laquelle nous pensons souvent, sans nécessairement effectuer de suivi pour voir comment cela aboutit.

Il est très utile, pour nous tous ici présents, de savoir que le Canada fait si bonne figure en matière de sécurité, par rapport à d'autres pays. C'était là un renseignement indispensable.

Quelqu'un a déjà posé la question, mais je suis restée un peu sur ma faim. Vous avez parlé de la capacité de la Direction générale de l'intégrité du Programme de passeport à effectuer des enquêtes administratives pour déterminer si la personne demeure admissible à un passeport ou à des services à l'avenir. Vous avez mentionné certaines des nombreuses raisons pour lesquelles on peut refuser un passeport à un individu. Vous avez parlé de l'incarcération, entre autres. Mais pendant combien de temps les gens perdent-ils leur droit à un passeport, quand cela leur arrive? Et comment font-ils pour en obtenir un, à supposer que ce soit même possible?

• (1245)

M. Peter Bulatovic: Je peux répondre à cette question.

La période de refus de service généralement imposée à un individu est de cinq ans, à compter de la date de l'incident. Nous prenons nos enquêtes administratives vraiment au sérieux.

Nous savons que la Charte garantit aux Canadiens le droit à la liberté de circulation. De ce fait, même durant la période de refus de service de cinq ans, nous laissons la personne faire une demande de passeport ponctuelle pour visiter de la parenté dans un autre pays pour des motifs d'ordre urgent, impérieux ou de compassion — et ce aussi souvent que souhaité durant la période de refus de service. Par contre, la personne ne peut pas avoir de passeport permanent durant la période de cinq ans.

Nous avons bien conscience du fait que les gens ont quand même besoin de voyager. Voilà pourquoi nous approuvons les demandes de passeport pour des considérations urgentes, impérieuses ou de compassion. Mais la période de refus de service dure généralement cinq ans.

Mme Tilly O'Neill Gordon: J'ai également été heureuse de vous entendre dire que la sécurité était bien mieux assurée grâce au nouveau passeport électronique. Est-ce le seul type de passeport qui sera distribué à compter de maintenant? Tous les gens qui font une demande désormais recevront-ils un passeport électronique?

M. Lu Fernandes: Oui. Le passeport électronique est désormais le seul passeport disponible pour les Canadiens, à compter du 1^{er} juillet 2013. La seule différence est la période de validité choisie pour le passeport: 5 ans ou 10 ans.

Mme Tilly O'Neill Gordon: D'accord. Est-ce qu'on doit maintenant se présenter à un bureau pour faire la demande? Parce que bien des gens n'auraient pas... Ou peut-on faire sa demande à partir de son propre ordinateur?

M. Lu Fernandes: On peut se rendre sur le site Web de Passeport Canada et remplir une demande en ligne, mais, à l'heure actuelle, il faut ensuite l'imprimer pour l'envoyer par la poste à Passeport Canada ou encore déposer le formulaire en personne à un bureau de Passeport Canada, de Service Canada ou de Postes Canada.

Mme Tilly O'Neill Gordon: Il n'est donc pas du tout nécessaire d'avoir un ordinateur ou de savoir comment s'en servir. Les Canadiens peuvent aller dans un bureau et obtenir le service de cette façon.

M. Lu Fernandes: Tout à fait.

Mme Tilly O'Neill Gordon: Je me demandais quelle est la meilleure chose que les Canadiens puissent faire pour lutter contre ces courriels hameçons, les logiciels malveillants et le réacheminement du trafic, parce que ces phénomènes se manifestent certainement de plus en plus chaque jour grâce à cette belle technologie à notre disposition aujourd'hui. Je me demande ce que les Canadiens peuvent faire pour prévenir tout ça.

M. Michael Jenkin: Eh bien, dans la trousse que nous vous avez remise, vous trouverez des suggestions pour vous protéger en ligne, surtout contre les tactiques d'hameçonnage et tout le reste.

Selon moi, le meilleur conseil à donner, c'est de faire très attention. La question fondamentale est celle-ci: ne révéler aucune information personnelle en ligne à moins de très bien comprendre à qui vous avez affaire. S'il s'agit d'une personne que vous connaissez et en qui vous avez confiance, c'est une chose, mais certainement, la

plupart des entreprises et institutions respectables ne vous demandent pas d'envoyer des renseignements personnels précieux à froid, en ligne.

Malheureusement, les criminels dans ce domaine s'en prennent souvent aux émotions. Par exemple, le stratège typique constitue en un courriel que vous recevriez et qui aurait l'air très officiel, d'une banque, par exemple, disant qu'il y a eu des problèmes avec son système de sécurité et votre compte et vous demandant de communiquer avec elle en ligne. Lorsque vous faites le contact en ligne — ou même dans certains cas, par téléphone, mais certainement en ligne —, on vous demande de présenter des renseignements personnels. Les banques ne procèdent jamais de cette façon.

Alors vraiment, il faut faire extrêmement attention aux situations dans lesquelles on fournit des renseignements personnels. On ne le fait que dans les circonstances où, par exemple, on fait légitimement une demande pour une pièce d'identité ou une carte de crédit, ou quelque chose de semblable. Mais il faut faire très attention aux demandes et aux instances reçues sans sollicitation, par hasard, dans lesquelles on vous demande des renseignements personnels de nature délicate. Il faut toujours faire preuve de prudence dans ces cas-là.

Autrement dit, si vous entreprenez les démarches, il n'y a pas de problème. Vous voulez faire une demande de carte de crédit, vous allez à la banque, vous remplissez un formulaire, etc. Mais lorsque quelqu'un communique avec vous par hasard, même si c'est la banque, et prétend qu'il y a eu un problème et qu'on a besoin de vos renseignements personnels, ne répondez pas. Allez directement à la succursale de votre banque pour demander s'il y a un problème, parce qu'il faut faire très attention lorsque des gens demandent des renseignements personnels de but en blanc. C'est ce qu'il faut se rappeler.

• (1250)

Mme Tilly O'Neill Gordon: Nous devons de plus en plus transmettre ce message et le faire comprendre afin que les gens ne se fassent pas avoir à la première occasion, parce qu'ils sont nerveux ou curieux de savoir quel a été le problème avec leurs transactions bancaires, si bien qu'ils donnent automatiquement de l'information qu'ils ne devraient pas divulguer. C'est un message très important que nous devons transmettre de plus en plus.

Le président: En fait, vous n'avez plus de temps; je suis désolé, Tilly.

Merci beaucoup.

Je remercie tous nos témoins. Voilà qui met fin à la période des questions.

Messieurs Fernandes, Bulatovic et Jenkins, vos exposés ont été très utiles, et nous aurons peut-être besoin de vos lumières plus tard au cours de notre étude. Nous n'hésiterons certainement pas à faire appel à vous au besoin.

Je vais suspendre la séance brièvement, après quoi nous siégerons à huis clos pour environ cinq minutes.

La séance est levée.

[La séance se poursuit à huis clos]

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

PERMISSION DU PRÉSIDENT

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 du Parlement du Canada à l'adresse suivante : <http://www.parl.gc.ca>

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

SPEAKER'S PERMISSION

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 Parliament of Canada Web Site at the following address: <http://www.parl.gc.ca>