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 020 • 2e SESSION • 41e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 1er mai 2014

Président

M. Pat Martin

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

Le jeudi 1er mai 2014

● (1145)

[*Traduction*]

Le président (M. Pat Martin (Winnipeg-Centre, NPD)): Je déclare la séance ouverte. Mesdames et messieurs, nous sommes en retard. Nous commencerons par présenter nos excuses aux témoins. Ce retard inévitable découle de la tenue d'un vote à la Chambre des communes.

Le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique se réunit donc afin de poursuivre son étude du problème grandissant du vol d'identité et de ses répercussions économiques.

Nous sommes heureux d'accueillir nos deux témoins, M. Avner Levin, un professeur agrégé à l'Université Ryerson, et Mme Éloïse Gratton, qui est associée et vice-présidente à la division de la Conformité, pour le cabinet McMillan LLP, à Montréal.

Soyez les bienvenus. Nous allons vous inviter à faire vos exposés. Toutefois, nous devrons nous en tenir à une seule série de questions de sept minutes pour chacun des partis. Cela devrait nous laisser assez de temps pour traiter de travaux du comité à la fin de la séance.

La parole est à vous. Vous pouvez le faire dans l'ordre que vous préférez.

Mme Éloïse Gratton (associée et vice-présidente, Conformité, McMillan LLP, à titre personnel): Je vais commencer. Merci de l'invitation.

[*Français*]

Je ferai la première partie de ma présentation en français et la deuxième en anglais.

J'aimerais d'abord discuter du cadre légal en matière de protection des renseignements personnels dans lequel évoluent les entreprises. Malgré le fait que nous ayons une loi en cette matière, soit la Loi sur la protection des renseignements personnels et les documents électroniques, ou LPRPDE, il n'y a aucun incitatif pour que les organisations et les entreprises se conforment à la loi et adoptent des mesures de sécurité adéquates. Quel est le pire des scénarios pour les entreprises? Quel risque courent-elles si elles ne se conforment pas à la loi? Ce n'est pas grand-chose. En fait, dans le pire des cas, elles risquent de voir leur réputation être ternie. Par exemple, si, à la suite d'une plainte, la commissaire fait une enquête et décide de nommer l'entreprise, celle-ci risque évidemment de voir sa réputation être entachée, mais cela n'arrive que très rarement.

Elles peuvent courir un autre risque. En effet, quand un individu reçoit une confirmation du commissaire qu'il y a eu une infraction à la loi, il peut s'adresser à la Cour fédérale pour demander des dommages-intérêts. Il y a eu quelques décisions à cet égard au cours des 10 dernières années. Cinq à dix décisions ont été rendues par la Cour fédérale en vertu desquelles on a accordé de petits montants. Parfois, il n'y a en aucun, parfois c'est 5 000 $.

Une décision a été rendue l'automne dernier dans la cause *Chitrakar c. Bell TV*. On a alors accordé un montant de 20 000 $ et c'était une première. Est-ce une nouvelle tendance? C'est peut-être le cas. L'avenir nous le dira. Chose certaine, tout le monde ne peut pas nécessairement entamer des poursuites pour obtenir de petits montants. Souvent, dans les cas d'atteinte à la vie privée, on parle de petits montants de 5 000 $ à 10 000 $. C'est une démarche laborieuse et ce n'est pas évident.

De plus, il n'y a pas, au fédéral, l'incitatif qui peut découler des recours collectifs en matière d'atteinte à la vie privée. Dans les autres juridictions, cela existe. Dans plusieurs cas, cela incite les entreprises à se conformer à la loi. Pensons aux failles relatives à la sécurité qui ont eu lieu. En janvier dernier, il y a eu un bris de sécurité à Ressources humaines et Développement des compétences Canada. En avril, il y eu un bris de sécurité à l'Organisme canadien de réglementation du commerce des valeurs mobilières, ou OCRCVM. En vertu de ces bris, des recours collectifs ont été intentés.

Simplement à titre d'exemple, dans l'affaire de l'OCRCVM, il était question d'un disque perdu qui contenait des renseignements financiers au sujet de 52 000 individus, clients de firmes de courtage. On réclame 1 000 $ par individu. Cela pourrait donc être un incitatif, mais ce n'est pas un véhicule possible en vertu de la LPRPDE. Il n'y a pas d'incitatifs pour les entreprises. Même si c'était possible, tout l'aspect du recours collectif n'est pas invitant car on n'obtient pas nécessairement l'autorisation.

Une décision a été rendue en 2010 dans la cause *Larose c. Banque Nationale du Canada*. C'était un cas typique, soit celui d'un portable perdu qui contenait des renseignements financiers de plusieurs clients. L'un des clients n'était pas heureux de cet état de chose. Il a poursuivi la Banque Nationale. Au stade de l'autorisation, le représentant du plaignant a dû arriver à démontrer que, à la suite du bris de sécurité dont la banque était responsable, il y avait en effet eu des personnes victimes de vols d'identité. La cour a précisé que la simple crainte d'être victime d'un vol d'identité n'était pas indemnisable. Elle n'aurait pas pu autoriser le recours s'il n'y avait pas eu de preuve qu'il y avait eu un vol d'identité.

Vous voyez donc combien la barre est haute. Ces recours ne sont pas évidents. Les indemnisations constituent de petits montants. Qu'est-ce qui reste en fin de compte? S'il n'est pas possible de réclamer un dédommagement pour la crainte d'être victime d'un vol d'identité à la suite d'un bris de sécurité, il ne reste pas grand-chose.

Revenons donc à la loi en matière de mesures de sécurité. On suggère aux entreprises d'adopter des mesures de sécurité qui correspondent au degré de sensibilité des renseignements. En matière d'impartition, on dit aux entreprises qu'elles demeurent responsables même si les renseignements sont confiés à un tiers et qu'elles doivent protéger les renseignements par voie contractuelle. Dans bien des cas, en pratique, je vois des entreprises qui vont dans l'infonuagique ou qui font de l'impartition. Elles ont un contrat et se ferment les yeux.

● (1150)

Je veux vous amener à considérer une disposition d'une loi québécoise que je trouve très intéressante. Elle donne une obligation additionnelle aux entreprises qui s'apprêtent à donner ou à transférer des renseignements à un tiers dans un contexte d'impartition. C'est l'article 26 de la Loi concernant le cadre juridique des technologies de l'information. On peut lire ce qui suit:

> Quiconque confie un document technologique à un prestataire de services pour qu'il en assure la garde est, au préalable, tenu d'informer le prestataire quant à la protection que requiert le document en ce qui a trait à la confidentialité de l'information et quant aux personnes qui sont habilitées à en prendre connaissance.

La personne qui donne le mandat et qui transfère les renseignements, que ce soit dans l'infonuagique ou quoi que ce soit d'autre, a l'obligation de dire au fournisseur de services comment il doit protéger les renseignements. Je pense que ce serait un type de disposition qui pourrait être utile dans notre loi.

Je travaille dans le domaine de la protection de la vie privée et de la protection des renseignements personnels. Dans le cadre de mon travail, j'ai un volet qui porte sur la prévention. On parle donc de services-conseils, de conformité, de formation, d'élaboration de politiques, etc. J'ai aussi un volet qui porte sur la gestion de crise. Il s'agit donc de la gestion des bris de sécurité, de l'assistance lorsqu'il y a des plaintes formulées aux différents commissaires à la vie privée et les recours collectifs en matière de vie privée. Il est rare que j'obtienne des mandats en matière de prévention sans que, au départ, il y ait eu une crise. C'est la preuve que les entreprises ne sont pas très sensibilisées à cet égard. Or, la loi est là. Est-on motivé à se conformer à la loi? Plus ou moins, car on attend qu'il y ait un bris de sécurité avant d'agir. Lorsqu'il y a une crise, c'est là qu'on se dit que cela a coûté cher et que c'est peut-être le temps d'investir en matière de prévention.

C'est aussi intéressant de constater toutes les ressources qui sont mises de l'avant en matière de conformité et de prévention avec l'entrée en vigueur de la nouvelle Loi canadienne anti-pourriel. C'est une loi qui est prise au sérieux. Elle comporte des dispositions en matière de responsabilité pour les administrateurs, les dirigeants et les employeurs. Comme il y a des pénalités très élevées, elle est prise au sérieux. Depuis qu'on a annoncé son entrée en vigueur, cette loi monopolise ma pratique presque à temps plein. Est-ce que le pourriel est un plus grand problème ou un plus grand fléau que les problèmes de bris de sécurité ou de vol d'identité? J'en doute. Alors pourquoi avons-nous la situation actuelle? Qu'attend-on pour motiver les entreprises à investir en matière de prévention?

J'ai un dernier point à aborder. Cette deuxième partie sera très brève.

Il y a des études qui indiquent que la plupart des bris de sécurité sont causés par des erreurs humaines. Il y a deux études sur lesquelles je me base et qui ont été réalisées deux ans après l'entrée en vigueur de l'obligation pour les entreprises de faire état d'un bris de sécurité. Premièrement, il y a le rapport de 2012-2013 de l'Alberta où les mentions à cet égard et les bris de sécurité ont été répertoriés. Il a été mentionné que, dans bien des cas, il s'agissait d'une erreur humaine. Il y a aussi un rapport de 2013 du Ponemon Institute qui mentionne que, dans 33 % des cas, il s'agit d'une erreur humaine de la part des employés.

Encore là, je trouve que les entreprises ne prennent pas au sérieux tout le volet impliquant la formation des employés. Dans bien des cas, il y a des bris de sécurité occasionné par un portable qui a été laissé dans une voiture. L'employé était-il au courant que cela pouvait constituer un risque? Y avait-il une politique à cet égard? Y avait-il une formation adéquate qui était offerte? Ce n'est pas clair.

● (1155)

[*Traduction*]

Je sais qu'il reste peu de temps. La deuxième partie est très brève.

Je veux soulever le fait qu'actuellement, en vertu de la LPRPDE, il n'existe aucune obligation de faire état d'un bris de sécurité, et je crois que cela pourrait bien avoir un rôle important dans la lutte contre le préjudice financier qui peut survenir dans le cas d'un vol d'identité résultant d'un bris de sécurité.

Si les personnes touchées sont avisées — qu'il s'agisse de consommateurs ou d'employés —, elles seront mieux placées pour se prémunir de dommages, comme le vol d'identité, car le fait d'avoir été informées les incitera à porter davantage attention à leurs états financiers, mensuellement ou quotidiennement, pour dépister toute transaction suspecte ou non autorisée. Ils surveilleront leur crédit par l'intermédiaire d'agences de notation comme Equifax et TransUnion. Cela incitera aussi les entreprises à établir d'entrée de jeu de meilleures pratiques en matière de sécurité des données.

Qu'en est-il de l'obligation de faire état d'un bris de sécurité à l'extérieur du Canada? Cela existe en Europe et aux États-Unis. La plupart des États américains ont des lois à cet égard. Au Canada, l'Alberta est, à ce jour, la seule administration à avoir une telle loi pour le secteur privé et les amendes imposées aux entreprises peuvent atteindre 100 000 $. Il a été observé que l'inclusion de l'obligation de faire état d'un bris de sécurité dans la loi a entraîné une augmentation du nombre de signalements des infractions en matière de sécurité et aussi une augmentation de la formation offerte dans le domaine de la protection des renseignements personnels. Les entreprises sont davantage portées et motivées à dépenser, car elles savent qu'elles seront tenues de faire état d'un bris de sécurité, le cas échéant.

Il faut un consensus au Québec. En 2011, la Commission d'accès à l'information du Québec a publié un rapport dans lequel on a fait ce constat. C'est une question de temps. Actuellement, on s'en remet à l'Assemblée nationale, mais sous peu, ce sera aussi obligatoire au Québec, espérons-le.

Au fédéral, plusieurs projets de loi ont été présentés: les projets de loi C-29, C-12, S-4 et C-475. Le plus récent est le projet de loi S-4. S'il est adopté, le projet de loi S-4 donnera-t-il des résultats? C'est mieux que rien, c'est sûr. Ce n'est peut-être pas parfait, mais c'est mieux que rien.

Je suppose que cela inciterait les entreprises à signaler les incidents. À mon avis, nous avons un rôle à jouer à cet égard. L'idéal serait de préciser les amendes qui seraient imposées pour tout manquement à l'obligation de signaler les bris de sécurité aux particuliers et aux commissaires à la protection de la vie privée. Il devrait être obligatoire de signaler un bris de sécurité dès que possible. J'hésite à fournir un délai précis parce que je me suis déjà retrouvée de l'autre côté. Parfois, en cas de bris, il faut d'abord mener une enquête avant de commencer à informer les gens et les commissaires à la protection de la vie privée, car il faut savoir ce qui s'est passé et ce qu'il faut divulguer ou non.

À mon avis, le commissaire à la protection de la vie privée devrait avoir le pouvoir d'ordonner à une entité de signaler un bris de sécurité à ses clients. Ces ordonnances doivent être rendues publiques et l'entité doit être nommée. Je pense que cela créerait l'incitatif nécessaire pour qu'elles consacrent des ressources financières aux mesures de prévention, ce qui serait utile pour atténuer le préjudice financier découlant d'un vol d'identité.

J'en suis à mon dernier point. Concernant l'obligation de faire état d'un bris de sécurité, ce ne serait pas une mauvaise idée que le Canada se dote d'une loi unique. En cas de bris de sécurité, divers systèmes pourraient être à risque. Je sais qu'il y a quelques années, la Conférence pour l'harmonisation des lois au Canada a rédigé l'ébauche d'une loi sur les avis d'atteinte à la protection des données. Cela pourrait être un outil utile.

Merci. Je pense que mon temps est écoulé.

Le président: En effet, madame Gratton. Toutefois, vous avez utilisé à bon escient le peu de temps dont vous disposiez. Merci beaucoup de cet exposé très utile.

Nous passons immédiatement à M. Levin. J'ai indiqué que M. Levin est un professeur agrégé, mais il est aussi président du département de droit et des affaires à l'École de gestion Ted Rogers. En outre, il est directeur du Privacy and Cyber Crime Institute à l'Université Ryerson. C'est un résumé plus complet de vos titres de compétence.

La parole est à vous, monsieur Levin.

● (1200)

M. Avner Levin (professeur agrégé, Ryerson University, à titre personnel): En effet, j'occupe de nombreuses fonctions.

Je remercie le comité de m'avoir aussi invité. Puisque je ne maîtrise pas le français comme le fait ma collègue, mon exposé sera entièrement en anglais. Je m'en excuse.

Aujourd'hui, j'aimerais vous parler du rôle des banques dans la lutte contre le vol d'identité et des répercussions croissantes du vol d'identité sur l'économie. Je vais d'abord vous parler d'une étude récente que mes collègues et moi avons faite sur une industrie en pleine croissance et sur les risques qu'elle présente. Il s'agit de ce que l'on appelle l'industrie des fournisseurs de services de regroupement. Ensuite, je traiterai brièvement du rôle des banques dans l'industrie des fournisseurs de services de regroupement. Pour terminer, sous un angle plus général, je parlerai des banques et de leur rôle.

Permettez-moi de commencer par notre recherche. Elle a été réalisée, sous la direction collègue de l'Université de Sherbrooke, M. Anastassios Gentzoglanis, grâce au programme de contributions du Commissariat à la protection de la vie privée du Canada. Je tenais à le souligner.

L'industrie des fournisseurs de services de regroupement est une industrie qui rassemble l'information financière d'une variété de sources pour le compte des clients. Si j'ai une carte de crédit émise par une banque, un compte de chèques dans une autre banque et un compte d'épargne dans une troisième, le fournisseur de services de regroupement recueille tous ces renseignements et je peux les consulter sur mon ordinateur de mon bureau, mon iPad ou, dans certains cas, mon téléphone. La recherche visait à connaître l'attitude des consommateurs à l'égard de ces services et — ce qui est plus important encore — à l'égard des mesures de sécurité mises en place par les fournisseurs pour les informations obtenues des clients, ainsi qu'à l'égard des problèmes de protection des renseignements personnels.

C'est un marché en croissance. Il existe actuellement sept entreprises dans ce secteur au Canada, mais ce ne sont pas nécessairement des entreprises canadiennes. Vous en connaissez peut-être quelques-unes de nom, comme Mint ou, pour certains, Quicken. Il y a Check, autrefois connue sous le nom de Pageonce. Il y a aussi Yodlee, Mvelopes et quelques autres. Dans le cadre de notre recherche, nous proposions de discuter en toute confidentialité avec ces entreprises, sans les identifier. Le but était de connaître leur fonctionnement, leurs mesures de sécurité et les garanties qu'elles mettent en place. Selon la LPRPDE, ce sont là des choses qu'elles devraient à tout le moins pouvoir fournir. Personne de l'industrie n'a accepté de nous parler de ces mesures.

Je crois que si elles avaient de bonnes mesures en matière de sécurité et de protection de nos renseignements financiers, elles n'hésiteraient pas à les divulguer. Cela leur ferait une bonne publicité. Or, personne de l'industrie n'a accepté de nous parler. La réponse que nous avons eue, c'est que le fait de nous parler ne présente aucun avantage. Nous trouvons cela très préoccupant et très troublant. Selon nos estimations, environ un million et demi de personnes au Canada — peut-être plus — utilisent ces services. On parle d'un public plus jeune, qui a un intérêt plus marqué pour ces services et qui est plus exposé aux risques. Cela suscite certaines interrogations par rapport à cette industrie.

Premièrement, quel organisme en assure la réglementation? Est-ce le BSIF, le Bureau du surintendant des institutions financières? Quel est le rôle de l'ACFC, l'Agence de la consommation en matière financière du Canada? Qu'en est-il du Commissariat à la protection de la vie privée? De qui relèvent ces entreprises? À qui rendent-elles des comptes? Ce ne sont pas des entreprises canadiennes. Par conséquent, elles ne considèrent pas nécessairement qu'elles sont visées par les exigences canadiennes.

Je vais brièvement parler du rôle des banques canadiennes par rapport à cette industrie précise. Les banques nous disent que les consommateurs doivent assumer tous les risques. Dans leur jargon, ils assimilent cette fonction à une transaction autorisée, ce qui signifie qu'elle est assujettie aux mêmes conditions qu'un achat par carte de crédit dans un magasin ou chez un autre fournisseur. J'autorise cette transaction; par conséquent, s'il y a un problème, j'en ai la responsabilité en tant que client.

Je pense que c'est aussi discutable, parce que j'estime que les banques devraient faire preuve d'une plus grande prudence par rapport à cette industrie et qu'elles devraient protéger davantage leur clientèle en leur offrant à la fois de l'information à ce sujet et des mesures en matière de sécurité et de protection des renseignements. Cependant, jusqu'ici, l'attitude des banques à l'égard des fournisseurs de services de regroupement est hostile, car elles considèrent que ces entreprises sont en quelque sorte leurs concurrents. Évidemment, de nos jours, toutes les banques offrent également des services mobiles et des services en ligne. Certaines d'entre elles songent à offrir des services de regroupement. Je pense que les consommateurs sont en quelque sorte oubliés, là-dedans. C'est l'un des problèmes que l'on observe par rapport à l'industrie des fournisseurs de services de regroupement.

Enfin, permettez-moi de parler brièvement des banques elles-mêmes. La question est de savoir si les banques ont un meilleur bilan en ce qui concerne le vol d'identité, la fraude d'identité et la fraude financière liée au vol.

● (1205)

Depuis plusieurs années, mes collègues et moi tentons d'obtenir des banques des informations sur le vol d'identité et les bris de sécurité liés au vol d'identité. Nous n'avons reçu aucune réponse. Nous avons demandé à chacune des banques. Nous avons demandé à l'ensemble des banques de nous fournir des informations par l'intermédiaire de leur association, l'Association des banquiers canadiens ou ABC.

Ce que nous voulions savoir correspond précisément à ce qui pourrait aider le comité dans ses travaux. Nous aimerions connaître les sources de fraude. Pouvez-vous nous fournir une ventilation par catégorie, par source ou par origine? Je vais vous donner quelques exemples. Quel pourcentage est attribuable aux pratiques des clients et consommateurs? Par exemple, nous avons vu récemment un reportage sur les mots de passe faciles au bulletin de nouvelles. Quel pourcentage des vols d'identité découle du fait que les gens utilisent des mots de passe faciles ou ne dissimulent pas leur numéro d'identification personnel correctement au guichet automatique ou à un terminal de point de vente? Quel pourcentage résulte de la négligence de gens qui gardent leur NIP dans une de leurs poches ou qui le mettent bien en évidence? Nous n'avons pas les réponses à ces questions.

En outre, quel pourcentage est attribuable à des criminels qui placent des dispositifs sur les guichets automatiques, par exemple, afin de voler les numéros d'identification personnels des gens? Qu'en est-il des personnes qui utilisent des copieurs de carte sur des terminaux de point de vente pour voler des informations? Quel pourcentage des crimes est lié à des petits criminels comparativement au crime organisé? Quel pourcentage résulte d'activités d'employés malhonnêtes, que ce soit chez un détaillant ou dans une banque? Quel pourcentage est lié à des pays étrangers, des pays d'où proviennent beaucoup d'activités criminelles, qu'il s'agisse des États-Unis, d'un pays d'Europe de l'Est, de la Russie, de la Chine ou d'un autre pays asiatique? En tant qu'universitaires, comment pouvons-nous déterminer les causes du vol d'identité et la fraude d'identité? Sans ces informations, comment le gouvernement du Canada et le Parlement pourront-ils mettre en place, à l'avenir, des politiques adéquates à cet égard?

Je voudrais simplement préciser que nous ne sommes pas des journalistes; nous ne voulons pas nous en prendre à une banque précise. Quand nous communiquons avec les banques, nous leur indiquons que nous sommes déterminés à préserver la confidentialité et que nous ne pointerons aucune banque du doigt. Nous avons de nouveau demandé à l'ABC de nous fournir des données en bloc, mais à notre connaissance, les banques ne divulguent même pas ces données à l'ABC. Nous sommes obligés de nous fonder sur les données qui ont été publiées. Or, elles remontent à 2012, à notre connaissance. Le site Web de l'ABC contient quelques informations, mais sans répartition par catégories. Certaines informations ont été fournies par le Centre antifraude du Canada; elles remontent au milieu de 2013. Ce sont les données les plus récentes que j'aie vues, mais il n'y a pas de ventilation par catégorie; ce sont des données globales. Cela ne donne aucune indication en vue de l'établissement d'une stratégie adéquate pour l'avenir.

D'après les discussions informelles que nous avons eues, nous savons qu'il y a des centaines voire des milliers d'incidents que les banques, à l'interne, considèrent comme problématiques. Je parle de milliers de cas par banque, par année. Nous ne connaissons pas la nature de ces incidents. S'agit-il toujours d'incidents graves? Nous ne le savons pas. Sont-ils liés au vol d'identité? Nous ne le savons pas. Un facteur quelconque a permis à la banque de prendre connaissance d'un incident et d'intervenir. Comme l'a dit ma collègue, s'agit-il d'infractions qui devront être signalées au commissaire ou aux consommateurs? Nous ne le savons pas. Nous n'avons pas de renseignements pertinents et de qualité à leur sujet, ni sur leurs répercussions sur l'économie ou sur nous.

Ces dernières semaines, avant de venir témoigner au comité, pour faire preuve de diligence raisonnable, nous avons communiqué de nouveau avec l'ensemble des banques. Comme je le disais, cela dure depuis plusieurs années. À ce jour, ni les banques ni l'ABC n'ont donné suite à nos demandes. J'estime que les banques ont un rôle clé à jouer. Elles doivent faire preuve de transparence. Elles doivent rendre des comptes. En tant qu'entreprise individuelle, aucune banque n'est tenue de se placer en position désavantageuse par rapport à ses concurrents du secteur bancaire. Toutefois, en tant que groupe, régler ce problème fait partie de ce que j'appellerais leur responsabilité d'entreprise.

● (1210)

J'exhorte le comité à demander aux banques de communiquer ces renseignements au public et aux universitaires, à tout le moins aux membres du comité, afin que vous ayez devant vous les renseignements nécessaires pour accomplir le travail important que vous avez entrepris.

Sur ce, je tiens à vous remercier tous. Je me ferai un plaisir de répondre à vos questions, si nous avons le temps.

Le président: Merci beaucoup, monsieur Levin.

Les questions que vous nous posez renforcent notre détermination à effectuer cette étude et confirment nos raisons de le faire. Je peux vous assurer que les banques devront comparaître devant le comité et qu'elles ne se défileront pas avec nous comme elles l'ont manifestement fait avec vous, je vous le garantis. Nous ferons tout en notre pouvoir pour nous assurer qu'elles répondent aux questions qui leur sont posées.

Malheureusement, nous n'aurons le temps de faire qu'un seul tour de cinq minutes chacun. Je pense que nous vous demanderons de revenir témoigner dans le cadre de cette étude — j'espère que tout le monde sera d'accord — probablement après que nous aurons entendu les banques à nouveau.

Nous allons commencer les questions en donnant la parole à l'opposition officielle.

MadameBorg, vous disposez de cinq minutes.

[*Français*]

Mme Charmaine Borg (Terrebonne—Blainville, NPD): Merci beaucoup, monsieur le président.

Effectivement, les témoignages que nous avons entendus étaient très intéressants. Je vais poser mes questions rapidement parce que je n'ai pas beaucoup de temps.

Deux semaines après que j'aie commencé à utiliser Mint, ma carte de crédit a fait l'objet d'une fraude. Je ne sais pas si c'est relié. Je vais peut-être me désabonner.

Vous avez dit voir un problème dans le fait que ces compagnies, parce qu'elles ne sont pas canadiennes, ne sont pas assujetties à nos lois. Néanmoins, elles mènent des activités au Canada. Quelles mesures notre comité pourrait-il proposer pour régler ce problème?

Mme Éloïse Gratton: Ces compagnies ne sont pas assujetties à nos lois, mais même si elles l'étaient, seraient-elles motivées à les respecter? Cela me ramène au premier point de ma présentation.

[*Traduction*]

Je ne sais pas si vous avez quelque chose à ajouter.

M. Avner Levin: Oui.

Je suis d'accord avec ma collègue. Pour ces questions, il faut un organisme de réglementation efficace et distinct, qui pourrait imposer des sanctions efficaces. Les banques réagissent de façon tout à fait différente selon qu'il s'agit du BSIF ou du Commissariat à la protection de la vie privée — sans vouloir leur manquer de respect — en raison des pouvoirs que possède chaque institution par rapport à elles. Si nous voulons agir sérieusement, je pense que nous devons déterminer quels pouvoirs nous donnerons à l'organisme de réglementation qui sera choisi.

Il nous faut un organisme de réglementation efficace, en particulier avec les petits acteurs. Les banques sont des entreprises établies qui ont des traditions. Les petits acteurs me préoccupent beaucoup également, car bien souvent, ils ne sont pas Canadiens et ils ne sont pas même conscients de devoir respecter les lois canadiennes.

[*Français*]

Mme Charmaine Borg: Merci.

Je vais poursuivre sur le même sujet.

Tous les deux, vous avez mentionné que nos lois n'avaient pas assez de mordant et que, par conséquent, il n'y avait pas assez de conséquences. De plus, la commissaire a très peu de pouvoirs pour rendre des ordonnances et imposer des sanctions pécuniaires.

Le projet de loi S-4 est-il une bonne solution à cet égard? Est-ce qu'il manque des aspects dans ce projet de loi? Si oui, qu'est-ce que ce projet de loi devrait contenir afin qu'on soit bien protégés?

Mme Éloïse Gratton: Vers la fin de ma présentation, j'ai mentionné quatre ou cinq points, mais je vais vous parler d'autre chose.

Idéalement, le défaut de rapporter un bris aux mesures de sécurité devrait entraîner des sanctions. Il faudrait que la commissaire ait le pouvoir de rendre des ordonnances et que celles-ci soient rendues publiques. Le risque lié à la réputation que pourraient courir ces entreprises, que ce soit des banques ou des compagnies de télécommunications, serait un bon incitatif à rapporter une atteinte aux mesures de sécurité.

Il est sûr qu'on pourrait décortiquer le projet de loi plus en détail. Le test du *real risk of significant harm*, soit le risque réel de préjudice grave est-il trop élevé? Est-il trop subjectif? Les entreprises ne vont-elles pas considérer que ce risque est difficile à évaluer dans les cas où les renseignements ont simplement été perdus, même si ce ne sont que des renseignements financiers?

Comment pourrait-on évaluer *the risk of misuse*, soit le risque de mauvaise utilisation des données? Ce n'est pas toujours clair. Donne-t-on trop de latitude aux entreprises relativement à ce critère? On pourrait y revenir et étudier cela plus en détail, mais il est sûr que c'est mieux que rien.

Mme Charmaine Borg: Monsieur Levin, voulez-vous ajouter quelque chose à ce sujet?

[*Traduction*]

M. Avner Levin: Je pense que les avocats parlent tellement de ce que signifie le préjudice réel et important que cela dépasse presque l'entendement. Selon moi, si l'on veut agir sérieusement, on doit donner à la commissaire le pouvoir d'ordonner aux entreprises d'agir. C'est ce qu'elle demande. D'autres commissaires provinciaux ont ce pouvoir.

Jusqu'ici, cela ne figure pas dans la version actuelle. Je crois que ce serait une excellente suggestion et un excellent amendement à proposer que de donner davantage de pouvoirs à la commissaire à l'avenir en ce qui concerne les entreprises privées.

● (1215)

[*Français*]

Mme Charmaine Borg: Merci.

C'est justement ce que j'avais proposé dans le projet de loi C-475 que j'ai présenté, mais les conservateurs ont voté contre. C'est bien dommage. Nous allons quand même continuer à essayer de faire adopter de telles mesures.

Me reste-t-il du temps, monsieur le président?

[*Traduction*]

Le président: Il vous reste environ une minute et demie.

[*Français*]

Mme Charmaine Borg: Monsieur Levin, j'aimerais revenir sur le manque de coopération dont vous avez parlé. J'ai trouvé ça vraiment intéressant.

Pourrait-on faire quelque chose pour encourager une meilleure collaboration entre les banques et les universitaires? Pourquoi ne veulent-ils pas coopérer? Est-il possible qu'ils n'aient pas ces données ou qu'il n'y ait pas de spécialistes qui sont en train de faire de telles analyses?

[*Traduction*]

M. Avner Levin: Je pourrais peut-être commencer.

Je pense que c'est exactement comme elles l'ont dit. Elles n'y voient aucun avantage. On pourrait divulguer de l'information à leur sujet qu'elles préfèrent ne pas connaître. Les universitaires aiment bien critiquer, et on revient toujours à cette crainte que des renseignements qui les mettraient mal à l'aise soient révélés. Le système mis sur pied par les banques du Canada pour les consommateurs permet que la plupart du temps, nous n'ayons pas de répercussions directes sur le plan financier, car lorsqu'elles conviennent que nous n'avons pas autorisé les transactions, elles assumeront les pertes liées à la fraude.

Lorsqu'on fait le calcul, cela ne représente pas un coût énorme pour les banques. Les banques disent deux choses: « Laissez-nous faire » et « Vous ne subirez aucune conséquence ». Je pense que c'est en quelque sorte leur double message. La question est de savoir si ce sera suffisant dans l'avenir, surtout étant donné qu'il est question dans les banques et d'autres pays d'augmenter la limite de responsabilité personnelle. Certaines personnes disent que leur responsabilité personnelle est fixée à 50 $ si la sécurité de leur compte est compromise. Je crois que ce sont là des questions très importantes pour l'avenir.

Le président: Monsieur Levin, je crains de devoir vous interrompre.

Charmaine, ces cinq minutes sont très vite passées. Merci.

C'est maintenant au tour de Laurie Hawn, pour les conservateurs.

L'hon. Laurie Hawn (Edmonton-Centre, PCC): Merci à vous deux d'être ici.

Je vais commencer par vous, monsieur Levin. J'ai un compte à la banque TD, mais j'ai une carte Visa de la CIBC. Dans les deux cas, ma carte de débit et ma carte de crédit ont été bloquées à divers moments. C'était ma faute, car j'avais oublié de les aviser que j'étais ailleurs, et un logiciel quelconque est intervenu après avoir détecté une anomalie. Même si ce fut assez embêtant à ce moment-là, je suis content que cela existe.

Vous parlez des banques, des avantages et des inconvénients, et des banques qui disent ne pas y voir d'avantage. S'il n'y a pas d'avantage pour elles, alors il doit y avoir des inconvénients. Cherchons-nous à les pénaliser davantage? Si le président de la Banque Royale du Canada vous dit qu'il n'y a pas d'avantage, qu'allez-vous lui répondre? Comment lui expliquez-vous l'avantage pour la banque?

M. Avner Levin: Encore une fois, je ne veux pas vraiment... Je pense qu'il ne serait pas très utile pour le Canada de nous attaquer à la Banque Royale, à la TD ou à la CIBC.

Je leur demanderais de nous dire quelles sont les sources de vol et de fraude d'identité. Selon elles, d'où vient le problème? Est-ce un problème interne lié à des employés malhonnêtes? Dans ce cas, nous vous dirons ce que vous devez faire à ce chapitre. Mais s'agit-il d'un autre type de problème? Par exemple, est-ce la responsabilité du consommateur? Est-ce seulement parce que j'ai oublié de leur dire que je me rendais quelque part? Nous devons savoir où trouver des pistes de solutions en fonction de ces informations. Ce qui pose problème, c'est que je n'ai pas les renseignements requis pour vous donner une opinion éclairée sur la meilleure chose à faire sur le plan des sanctions.

L'hon. Laurie Hawn: Savez-vous si les banques se parlent entre elles? Selon moi, l'avantage, c'est leur coopération, car je suis sûr qu'elles ont toutes les mêmes problèmes.

M. Avner Levin: Elles ont le même problème, mais à ma connaissance, elles n'en parlent pas entre elles. Elles considèrent qu'il s'agit d'une vulnérabilité, alors elles parlent généralement des enjeux, mais elles ne partagent pas vraiment cette information. Je crois qu'elles n'en parlent même pas de façon anonyme à l'ABC.

L'hon. Laurie Hawn: Il me semble que ce serait un avantage.

Madame Gratton, nous avons parlé du risque, des conséquences et du manque de planification. Elles attendent qu'une crise survienne, puis elles courent dans tous les sens. Si nous augmentions le risque ou les conséquences, cela les inciterait-il à faire preuve d'un peu plus de sérieux dans la planification préliminaire?

Mme Éloïse Gratton: Je le crois. La Loi anti-pourriel, ou LCAP, qui entrera bientôt en vigueur, en est un excellent exemple. Les gens la prennent très au sérieux. L'incitatif est là si les sanctions y sont; il y a la responsabilité des administrateurs et des dirigeants, la responsabilité des employeurs, et les gens sont d'accord. Je crois donc que oui.

L'hon. Laurie Hawn: Du côté des petites réclamations, les recours collectifs semblent populaires; de toute évidence, l'union fait la force. Est-ce le meilleur outil pour ce genre de choses? Les gens sont manifestement incités à suivre le mouvement.

Mme Éloïse Gratton: Oui, un peu. C'est encore difficile sur le plan des autorisations, bien que depuis un an, nous ayons eu deux cas, un contre Apple au Québec, qui a été autorisé l'été dernier, et un autre concernant la Loi sur la protection des renseignements sur la santé de l'Ontario, l'affaire Kay, qui a été autorisé.

Ils sont de plus en plus autorisés et de plus en plus nombreux. Au moins, cela crée un incitatif.

Je pense qu'il est intéressant d'examiner l'affaire concernant la Banque Nationale et LaRose, dans laquelle le tribunal a indiqué qu'il n'autoriserait le recours que si le plaignant démontrait qu'il avait été victime d'un vol d'identité à la suite du bris de sécurité. Comment peut-on démontrer cela? Il est parfois difficile d'établir un lien entre le bris et les dommages.

● (1220)

L'hon. Laurie Hawn: Avez-vous examiné les statistiques relatives à cette question précise? Combien de personnes en ont réellement été victimes, et combien ont simplement suivi le mouvement parce que cela semblait être une bonne idée à ce moment-là?

Mme Éloïse Gratton: Eh bien, au Québec, nous avons un système de retrait, alors personne ne suit aveuglément le mouvement comme tel, mais effectivement, vous avez raison. Il y a des avocats qui gagnent leur vie en déposant des recours collectifs pour atteinte à la vie privée, parfois des copies de dossiers des États-Unis qu'ils importent ici. Il nous arrive de défendre ces affaires; nous agissons à titre d'avocats de la défense.

M. Avner Levin: Si on examine les données publiées par la GRC ou les gens qui signalent les fraudes aux diverses organisations — et il y a un an, je crois que la valeur combinée était d'environ 17 millions de dollars — et qu'on les compare à la valeur combinée que les banques et les sociétés émettrices de cartes de crédit déclarent, soit environ 440 millions de dollars, on peut voir la différence entre ce que les gens déclarent eux-mêmes et ce que les banques estiment. Encore une fois, nous ne savons pas ce qui explique cet écart et ce qui a causé toute cette fraude, si l'on veut, au-delà des 17 millions de dollars, et d'où cela provient.

L'hon. Laurie Hawn: En quoi avez-vous le plus confiance: les données des banques ou les données de la GRC?

M. Avner Levin: La GRC dit en quelque sorte que les gens ne le signalent tout simplement pas. Si on le lui demande, elle dira que les gens ne le déclarent pas, qu'ils se sentent gênés, que cela ne vaut pas la peine, etc.

L'hon. Laurie Hawn: Madame Gratton, vous avez parlé de l'article 26 de la loi québécoise. Cela semble logique. Dans quelle mesure la personne qui transfère les renseignements est-elle responsable de s'assurer que ceux qui les reçoivent comprennent bien leurs responsabilités en matière de protection?

Mme Éloïse Gratton: Eh bien, c'est un peu flou, non? Il y a un contrat, dont le libellé dit habituellement dans des termes très généraux qu'ils doivent protéger les renseignements conformément aux lois applicables.

Ils veulent simplement faire des affaires. Ils veulent le contrat. Ils le signeront. Au bout du compte, quel genre de chiffrement utilisent-ils? Où les données seront-elles stockées? On ne tient pas nécessairement compte de tous ces facteurs; c'est pourquoi j'aime bien cet article de la loi québécoise, qui crée une obligation additionnelle pour l'auteur du transfert.

L'hon. Laurie Hawn: C'est cela. Je voulais dire l'auteur du transfert.

Le président: Laurie, votre temps est écoulé. Merci beaucoup.

Merci, madame Gratton.

C'est maintenant au tour de Scott Andrews, du Parti libéral.

M. Scott Andrews (Avalon, Lib.): Soyez les bienvenus.

Madame Gratton, au début de votre exposé, vous avez parlé de la commissaire à la protection de la vie privée et des pouvoirs d'application de la loi. Pourriez-vous nous donner une idée des pouvoirs d'application de la loi que nous devrions lui accorder? Peut-être pourriez-vous nous en dire un peu plus sur les amendes et les pénalités, ainsi que sur les seuils acceptables, selon vous, qu'elle pourrait mettre en oeuvre.

Mme Éloïse Gratton: Ils ne devraient pas être inférieurs à ce que prévoit la LCAP, n'est-ce pas? Les pourriels sont un problème. La vie privée et le vol d'identité sont aussi un problème; pourquoi les seuils devraient-ils être inférieurs, alors? Si elle avait le pouvoir d'imposer des amendes de millions de dollars ou de centaines de milliers de dollars, je crois que cela inciterait les entreprises à prendre cette loi au sérieux.

Si l'on ajoute la responsabilité des administrateurs et des dirigeants et la responsabilité des employeurs, je pense que nous avons là un ensemble complet.

M. Scott Andrews: Vous avez parlé des entreprises qui confient des renseignements à un tiers. Pourriez-vous nous en dire plus à ce sujet? Pourriez-vous nous citer des exemples de situations où un problème survient ou nous dire à quel moment il survient? Est-ce quand le tiers a les renseignements et qu'à la fin du contrat, il ne les élimine pas? Avez-vous des exemples? Pourriez-vous nous en parler plus en détail?

Mme Éloïse Gratton: Oui. Parfois, ils ne sont pas déchiquetés. Ils sont stockés. De plus, on ne procède pas au déchiquetage numérique... Il y a du matériel électronique dans lequel les données ne sont pas effacées qui est fourni à un autre employé, à un autre client... Il y a eu l'affaire concernant Bureau en gros.

J'ai vu un cas récemment où les renseignements ont été perdus en transit. Il s'agissait de renseignements financiers. Qui est responsable? Est-ce le service de messagerie? Au bout du compte, c'est un peu tout le monde... L'entreprise est responsable des renseignements qu'elle a remis au service de messagerie, mais c'est le service de messagerie qui les a perdus. Pourquoi les a-t-il perdus? Parce que le bordereau d'expédition s'est détaché.

Il y a beaucoup de raisons différentes et divers types d'atteintes à la sécurité des données. Dans bien des cas, comme je l'ai dit, il y a erreur humaine. On laisse un ordinateur portable sur le toit d'une voiture ou on l'oublie à l'aéroport. Il y a beaucoup de cas d'erreur humaine. Je dirais qu'il y a toutes sortes d'atteintes à la sécurité des données.

● (1225)

M. Scott Andrews: S'il s'agit pour la plupart d'erreurs humaines, il n'y a pas d'intention malveillante; comment peut-on imposer des sanctions pour une erreur humaine?

Mme Éloïse Gratton: C'est une bonne question. Habituellement, la première chose que l'on vérifie, c'est si l'organisation avait mis en place des politiques appropriées et, dans l'affirmative, si les employés étaient au courant de ces politiques. Avaient-ils reçu une formation adéquate concernant la protection de la vie privée? Habituellement, si ces deux questions ont été réglées, si des mesures techniques et des politiques étaient en place et si les employés étaient au courant, cela limite clairement le risque. Ce n'est pas un système parfait et à toute épreuve, mais on limite clairement le risque.

M. Scott Andrews: Merci.

Monsieur Levin, j'aimerais que nous discutions un peu de ce que M. Hawn a mentionné tout à l'heure, soit que les banques bloquent nos cartes de crédit quand nous voyageons, et ce genre de choses. C'est en quelque sorte un système de détection précoce du vol d'identité, quand quelqu'un utilise vos cartes sans... À votre avis, comment les banques se débrouillent-elles à ce chapitre? Font-elles preuve de diligence raisonnable? Leur conduite est-elle acceptable à cet égard? Y a-t-il des études qui montrent qu'en fait, elles accusent beaucoup de retard et qu'au moment où elles en arrivent là, le mal est déjà fait?

M. Avner Levin: Sincèrement, je n'en ai aucune idée. Les banques refusent de dire quoi que ce soit sur leurs pratiques ou leurs politiques aux universitaires. Ce serait de la spéculation si je vous disais que les banques se débrouillent bien avec leurs algorithmes dans le cas de leurs clients qui sont partis à l'étranger et à qui on a oublié de dire que les cartes ont été bloquées. Je ne saurais vous dire si c'était des actions bien ou mal pensées. Nous ne détenons pas de renseignements sur le volume de fraude commise et pourquoi, et ce, en raison de tous les autres facteurs.

Nous avons un chiffre global. Pour 2012, il s'agissait d'un total de 440 millions de dollars déclarés par les banques et les sociétés de cartes de crédit. Nous ne disposons d'aucune ventilation quant aux causes et aux incidents.

Je suis désolé, mais je ne peux vous fournir d'avis pondéré sur le succès des banques dans ce domaine.

M. Scott Andrews: Nous avons parlé des agences de notation avec les autres témoins, et je crois que le témoignage des agences sera important. Ce sont ces gens qui peuvent déterminer quand la fraude commence.

Pensez-vous que les banques ont un rôle à jouer pour déterminer quand le vol d'identité vient de commencer? Croyez-vous qu'elles ont les compétences nécessaires, ou est-il trop tard, du temps que quelqu'un se rende dans une institution financière, d'essayer d'arrêter le vol de l'identité de la personne?

M. Avner Levin: Je crois que les banques peuvent le faire. Nous ne devons pas uniquement nous fier aux agences de notation. Les banques en sont capables, car ce sont elles qui appliquent les algorithmes. Ainsi, votre carte de crédit sera refusée si vous oubliez d'indiquer à la banque que vous êtes parti à l'étranger. Si les banques ont ce que nous appelons les faux positifs, elles devraient être en mesure de repérer les occurrences de fraude réelle au fur et à mesure que la fraude est commise et ainsi être beaucoup plus réactives.

Tous ceux qui sont passés par leur banque en cas de fraude savent que les banques sont extrêmement réticentes. La victime cherche souvent à savoir où la fraude a été commise, ce que le fraudeur a fait, ce qui est arrivé et dans quel magasin. Je peux vous dire que personne n'obtient ces renseignements de la banque. La banque donne comme prétexte des mesures de sécurité, car elle ne veut pas...

Le président: Monsieur Levin, je regrette, mais je dois vous arrêter.

Monsieur Andrews, votre temps s'est écoulé.

Nous avons en dernier lieu Mme Pat Davidson, du côté des conservateurs, qui dispose de cinq minutes.

Mme Patricia Davidson (Sarnia—Lambton, PCC): Merci beaucoup à vous deux d'être venus cet après-midi. Nous avons appris certaines choses fort intéressantes.

Monsieur Levin, pouvez-vous m'expliquer le mandat principal et les activités essentielles du Privacy and Cyber Crime Institute?

M. Avner Levin: Bien sûr.

Mon université utilise le mot institut pour fournir un cadre aux universitaires qui souhaitent effectuer de la recherche sur divers projets. Notre mandat vise les domaines de la protection de la vie privée et de la cybercriminalité.

De temps en temps, nous travaillons sur des projets qui portent davantage sur la protection de la vie privée et des renseignements personnels. Nous menons également des projets qui portent sur la cybercriminalité. C'est selon les professeurs et leurs intentions. Nous avons effectué des projets sur la protection de la vie privée en milieu de travail, en ligne et dans les médias sociaux. D'autres projets portent sur la publicité en ligne ou divers autres sujets qui intéressent nos membres. Notre rôle consiste à leur fournir un soutien administratif.

● (1230)

Mme Patricia Davidson: J'aimerais savoir quelles sont les causes les plus probables du vol d'identité. S'agit-il surtout de vol de données sur papier ou en ligne? Êtes-vous en train de me dire que vous n'êtes pas en mesure de nous le confirmer aujourd'hui parce que vous n'êtes pas capable d'obtenir ce type de renseignement?

M. Avner Levin: Tout à fait. Nous avons tenté de monter des projets de recherche sur ces questions précisément et, pour ce faire, nous cherchions à obtenir des renseignements auprès des banques. Nous étions prêts à signer tous les documents possibles pour garantir l'anonymat et la confidentialité des renseignements.

Nous, les universitaires, comme je l'ai dit, ne sommes pas des journalistes et ce n'était pas une question de recueillir un maximum de données; en général, nous communiquons nos rapports aux gens qui participent au projet, afin qu'ils puissent constater que nous avons tenu entièrement et fidèlement compte de leurs points de vue. Nous ne montrons quiconque du doigt et nous n'attribuons aucun blâme. Nous donnons à tous la possibilité d'intervenir à l'étape de la rédaction de l'ébauche du rapport. Les personnes peuvent ne pas être d'accord avec nos conclusions, mais elles ont certainement l'occasion de constater que leur point de vue a été repris fidèlement. Cependant, nous n'avons pas réussi à faire participer les banques, ni les fournisseurs de services de regroupement.

Mme Patricia Davidson: Aurais-je raison de dire que vous ne pouvez pas vous prononcer sur les victimes primaires du vol d'identité? Vous n'avez pas pu quantifier la fraude liée à l'identité et les problèmes connexes.

M. Avner Levin: Vous avez raison. Je n'ai pas pu le faire.

Mme Patricia Davidson: Madame Gratton, vous avez parlé de la Loi sur la protection des renseignements personnels et les documents électroniques. En 2007, une fiche de renseignements sur les entreprises et le vol d'identité a été publiée, dans laquelle le Commissariat à la protection de la vie privée a noté ce qui suit: « Il est possible de déduire les risques de vol d'identité en intégrant les principes fondamentaux de protection des renseignements personnels prévus dans la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) au sein de la culture des organisations. »

Pensez-vous que les organisations touchées par le vol d'identité suivront cette recommandation?

Mme Éloïse Gratton: Certaines le font, d'autres pas.

Mme Patricia Davidson: Celles qui le font, ont-elles constaté une différence?

Mme Éloïse Gratton: Certainement, mais parallèlement, les organisations qui se conforment à la loi commencent à se fâcher du fait que d'autres ne le font pas. Hier, on a parlé des sociétés de télécommunications qui divulguaient des renseignements personnels. J'ai reçu un appel d'un de mes clients qui disait: « Sommes-nous la seule société de télécommunications qui ne divulgue pas de renseignements personnels? Notre secteur commence à se faire une mauvaise réputation et nous obéissons à la loi. Ce serait plus facile de tout simplement fournir les renseignements personnels. » Essentiellement, certaines organisations s'y conforment, d'autres pas.

Mme Patricia Davidson: Si l'on ne dispose pas de renseignements sur les éventuelles victimes, comment peut-on savoir qui obéit à la loi et qui ne le fait pas? Comment?

Mme Éloïse Gratton: C'est un défi, mais je crois que nous en saurons davantage si on impose l'obligation de signaler. Si une succursale ou une unité recueille les renseignements ainsi que les signalements et est en mesure d'indiquer que ce type d'atteinte se produit dans le pays, nous pourrons en brosser un tableau plus exact.

Mme Patricia Davidson: Y a-t-il des mesures particulières que les organisations peuvent prendre afin de prévenir plus efficacement la fraude?

Mme Éloïse Gratton: De plus en plus souvent, j'inclus dans les contrats des dispositions concernant le droit à une vérification. C'est facile de dire qu'on va bien protéger les renseignements, c'est toute une autre paire de manches d'accorder à autrui le droit de venir vérifier sur les lieux, de fouiller les serveurs, de déterminer comment les données sont stockées. J'inclus ce type de dispositions de plus en plus souvent dans les contrats, notamment les contrats sur les services informatiques en nuage. C'est une façon de résoudre le problème.

Le président: Pat, je dois vous interrompe. Cinq minutes se sont écoulées.

C'est la fin de la période de questions. Je regrette de devoir vous arrêter, car nous sommes bien chanceux de pouvoir recueillir les témoignages de deux lumières comme vous.

Nous vous sommes très reconnaissants et vos témoignages nous seront d'une aide précieuse. J'espère que nous aurons l'occasion de vous entendre une autre fois, si les membres du comité l'estiment utile après que nous aurons reçu les agences de notation et les banques.

Merci beaucoup d'être venus aujourd'hui.

Nous allons lever la séance quelques instants pendant que les témoins quittent la salle, et nous reprendrons ensuite à huis clos pour discuter des futurs travaux.

[*La séance se poursuit à huis clos.*]