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 033 • 2e SESSION • 41e LÉGISLATURE

TÉMOIGNAGES

Le lundi 23 février 2015

Président

M. Pierre-Luc Dusseault

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

Le lundi 23 février 2015

● (1530)

[*Français*]

Le président (M. Pierre-Luc Dusseault (Sherbrooke, NPD)): Bonjour à tous et bienvenue à la 33e séance du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. Nous poursuivons aujourd'hui notre étude sur le problème grandissant du vol d'identité et ses répercussions économiques.

Il y a quelques mois, plusieurs témoins ont comparu devant nous pour traiter de cet enjeu très important. Nous allons maintenant entendre deux témoins qui vont nous entretenir de cette question. Chacun des témoins va disposer de 10 minutes pour livrer sa présentation. Les membres du comité pourront ensuite leur poser des questions.

Nous allons d'abord entendre, en direct et par vidéoconférence, Mme Sherbanowski, qui est directrice générale de la Crime Prevention Association of Toronto. Par la suite, je vais céder la parole à un invité que nous entendrons en direct d'Orlando, en Floride, soit M. Claudiu Popa, qui est pour sa part président-directeur général d'Informatica Corporation.

Je remercie nos deux témoins du temps qu'ils nous accordent aujourd'hui.

Madame Sherbanowski, vous avez la parole pour un maximum de 10 minutes.

[*Traduction*]

Mme Janet Sherbanowski (directrice générale, Crime Prevention Association of Toronto): Je vous remercie de me donner l'occasion de comparaître devant le comité.

La Crime Prevention Association travaille avec les consommateurs, les municipalités et les gouvernements depuis plus de 30 ans. Notre rôle consiste principalement à protéger les intérêts des gens et de la population. Nous travaillons beaucoup auprès des sociétés et du secteur privé, mais surtout des groupes de consommateurs et des personnes qui sont entrées en contact avec des gens qui ont peut-être volé ou utilisé leur identité, ou qui craignent d'être dans une situation à risque.

Pour vous donner un aperçu, je peux vous dire que nous en serons à notre troisième année de collaboration avec le Bureau de la concurrence et un groupe de Toronto, et la Commission de services policiers de Toronto sur la fraude et des questions connexes.

Le 20 mars, c'est notre journée « Changez votre NIP ». L'objectif est de faire en sorte que les gens pensent à changer leur NIP, leur numéro d'identification personnelle. C'est très difficile pour les gens de le faire parce qu'ils connaissent leur numéro par coeur. Il correspond au nom de leur chien, à l'anniversaire de leur mère ou à l'année de naissance de leur grand-mère, par exemple. Chaque année, nous suggérons donc aux gens d'ajouter un chiffre qui correspond à l'année, par exemple, si le NIP était 1886, ce serait 18865 cette année. C'est très populaire et utilisé par d'autres groupes de prévention du crime au pays. Nous sommes très fiers de pouvoir faire en sorte que les gens pensent à la protection de leur identité.

Comme je l'ai dit, nous collaborons également avec le Bureau de la concurrence. Nous travaillons avec le groupe fédéral chaque année.

Nous tenons des ateliers destinés aux nouveaux immigrants et aux aînés dans le cadre du programme Nouveaux Horizons pour les aînés. Nous tenons aussi maintenant ce type d'ateliers en collaboration avec le gouvernement de l'Ontario; nous travaillons auprès des nouveaux immigrants et des groupes jeunesse pour les aider à comprendre ce que sont la fraude en matière de crédit et la fraude d'identité et les informer sur les différents risques au Canada.

Nous collaborons avec la Banque Royale et la Banque Scotia, qui ont parrainé le programme ABCs of Fraud pendant un certain nombre d'années et qui ont fourni des fonds à ce groupe partout au Canada. Le groupe ne reçoit plus ces fonds depuis 2011. Cela fait quatre ans que nous offrons le programme en tant que groupe de bénévoles.

Nous collaborons avec un certain nombre de gens sur différentes questions: stratagèmes de rencontre, fraudes hypothécaires, achat de condo, faux mariages, etc. Le jour où j'ai reçu l'invitation de me joindre au groupe, une dame m'a envoyé un courriel. Dans un nombre croissant de cas, il s'agit d'escroqueries liées à l'emploi et d'utilisation frauduleuse des renseignements et de l'identité d'une personne. La dame m'a envoyé un courriel. Elle avait posé sa candidature à Service Canada. Normalement, toute information transmise à cet égard devrait passer absolument par la fonction publique. Elle a reçu un courriel d'un groupe qui est en fait une agence de voyages qui organise des pèlerinages. On lui demandait de fournir des références et un document de vérification de casier judiciaire. La dame en question m'a envoyé un courriel pour obtenir mon avis à ce sujet. Je lui ai dit que nous enverrions l'information à la GRC en son nom et avec sa permission, car c'est le type de renseignement qui peut être de plus en plus utilisé, pas nécessairement pour faire de la fraude financière, mais l'identité de la dame pourrait servir à créer une identité pour une personne qui se livre à des activités terroristes.

Un certain nombre de problèmes surgissent même dans l'industrie de consommation où l'identité d'une personne peut être utilisée sans qu'elle le sache. Nous nous rendons compte que de plus en plus, dans les cas où l'information est envoyée par courriel concernant des problèmes de chômage, qui sont grandissants, il est très facile de prendre l'information d'une personne et de créer une fausse identité.

● (1535)

Dans un certain nombre de cas, les fraudeurs ont le numéro d'assurance sociale. Ils savent où la personne a vécu, a fait ses études et a travaillé. Dans ce cas, lorsqu'une personne leur demande des renseignements — références et document de vérification du casier judiciaire —, le type de renseignements fournis permet aux gens de créer un très bon profil et de commettre non seulement une fraude financière à l'aide de l'information, mais peut-être aussi un acte encore plus vil.

En Ontario, notre association a travaillé avec le commissaire à la protection de la vie privée pour déterminer quelle information nous pourrions fournir aux consommateurs sur la protection de leur identité et de quelle façon nous pourrions leur signaler que les données massives et la façon dont les données sont extraites par les sociétés, et peut-être par le gouvernement, posent un risque. Ainsi, les consommateurs peuvent savoir que lorsqu'on leur demande des renseignements autres que des renseignements personnels ou des renseignements qu'ils hésitent à fournir, ils peuvent demander ce qu'ils devraient fournir et où l'information sera utilisée.

À notre point de vue, les consommateurs devraient être prévenus, par exemple, lorsque des institutions financières ne déclarent pas les atteintes à la protection des renseignements ou les vols de données sur les cartes de crédit ou de débit. La non-déclaration de ces actes nuit à l'augmentation de nos services de surveillance et peut-être à l'embauche d'un plus grand nombre de personnes dans les services de police ou du gouvernement pour l'examen de ces problèmes. Nous nous sommes penchés sur certains de ces problèmes pour ce qui est d'essayer de protéger les consommateurs dont la confiance en notre capacité à les protéger et de protéger leurs renseignements s'effrite. Ces gens n'ont pas l'impression que les services gouvernementaux ou d'autres fournisseurs de services tiennent compte de leurs intérêts, et c'est même le cas lorsqu'ils postulent à un emploi, comme nous le montre le cas de la dame qui m'a envoyé le courriel.

L'un des autres aspects dont il faut parler, c'est l'exploration de données dans le marché de détail pour trouver de l'information afin, par exemple, d'envoyer une paire de souliers à une personne, qui devra la retourner. On se fait prendre par un phénomène que nous observions dans les clubs de livres il y a des années. On envoie des produits à une personne parce qu'elle a choisi un type de service et, ce faisant, elle est exposée à bon nombre d'autres services et elle paie pour ces services sans savoir que cela faisait partie de son adhésion.

Je fais partie de plusieurs groupes qui se penchent sur la protection des renseignements. Aujourd'hui, j'ai reçu une demande de la part d'un groupe qui consistait à évaluer un programme qu'une société de recherche offrira dans des écoles. Dans le cadre du programme, on demandera aux enseignants ou aux conseils scolaires de suivre les activités des enfants. À mon avis, les renseignements recueillis seront également utilisés par des compagnies d'assurance, des institutions financières ou des organisations de gestion de l'information sur la santé pour déterminer si des gens seront admissibles à des produits liés à la santé plus tard. Si l'on recueille des renseignements sur l'activité physique d'un jeune à partir de la première année ou de la maternelle jusqu'à la douzième année en utilisant ce type d'application, 20 ans plus tard, une organisation de gestion de l'information pourrait dire à la personne « eh bien, puisque vous n'avez pas fait assez de sport, vous n'êtes pas admissible à un programme destiné aux diabétiques ».

● (1540)

Donc, à l'heure actuelle, pour un certain nombre de problèmes, on ne parle plus seulement de vol d'identité, mais aussi d'utilisation de l'identité. En ce qui concerne la protection de la vie privée, la collecte de données massives et l'utilisation des données, à cette étape-ci de notre histoire, nous avons la possibilité de mettre au point une bonne évaluation du risque pour les consommateurs.

C'est tout. Merci.

[*Français*]

Le président: Je vous remercie beaucoup de votre présentation.

Sans plus tarder, je vais céder la parole à M. Popa, président-directeur général d'Informatica Corporation, une entreprise qui fournit des logiciels et des services d'intégration de données. Il se joint à nous par téléconférence. Je le remercie de sa comparution. Son expérience nous aidera à aborder ce problème grandissant qu'est le vol d'identité.

Monsieur Popa, vous avez la parole.

[*Traduction*]

M. Claudiu Popa (président-directeur général, Informatica Corporation, à titre personnel): Je vous remercie encore une fois de m'avoir invité. J'en suis ravi.

Je m'appelle Claudiu Popa. J'ai un cabinet-conseil en gestion de risque à Toronto. Nous offrons des conseils sur la sécurité et la confidentialité.

Nous menons nos activités à l'échelle nationale dans la plupart des secteurs. Nous faisons des vérifications. Nous fournissons des services d'évaluation des risques concernant la confidentialité et la sécurité, de même que sur le plan de la continuité opérationnelle. Nous évaluons la normalisation des approches protectrices dans les organismes privés et publics, de sorte que nous avons un accès privilégié à ce que font les organismes. Bien entendu, nous regroupons une partie de l'information simplement pour avoir notre propre point de vue sur notre industrie.

Toute l'information portant sur nos engagements et nos clients est, par défaut, confidentielle. Nous examinons les tendances que nous pouvons observer et nous menons des recherches. Nous publions des livres blancs, des ouvrages. Nous tenons des séminaires et des activités d'information pour diffuser une partie de ces renseignements.

L'un de mes derniers ouvrages qui a été publié cette année porte sur la cyberfraude et la taxinomie à cet égard, dont le monde a grandement besoin, je crois.

En ce qui concerne le problème mondial que constitue la cyberfraude, nous constatons que de grandes tendances se dessinent dans le monde dans bien des cas, et dans la plupart des cas, avant même que le Canada soit touché. Il y a donc un aspect prévisionnel/dimension de prévision dans cela que nous essayons de mettre en évidence dans la publication.

Nous dégageons un certain nombre de tendances mondiales de différents types, mais il semble qu'il y a très peu de taxinomie et de définitions communes, surtout pour ce qui est de la collaboration des forces de l'ordre.

Nous savons qu'en ce qui concerne le vol d'identité, le problème prend de l'ampleur, mais surtout, nous croyons qu'il se transforme, et nos recherches sur les atteintes nous indiquent malheureusement que partout dans le monde, je dirais, on trouve de nouvelles façons de commettre ces crimes chaque année.

Nous avons tous vu les études qui ont été publiées par Intel et McAfee dans le cadre de leur rapport de 2014 sur la cybercriminalité dans le monde, qui indiquent que la cybercriminalité entraîne des pertes pouvant atteindre 575 milliards de dollars, dont une grande partie — et selon l'indice du taux d'atteintes de l'an dernier, dont la plupart — résulte de la compromission de milliards de dossiers individuels, et je ne parle que de l'année dernière.

Nous constatons que le Canada n'est pas le seul pays à subir les dommages. C'est un phénomène mondial. Nous sommes les premiers à avoir cerné les répercussions sur les individus, et ce sont eux qui sont touchés au bout du compte, car ils sont innocents. Bien entendu, dans bien des cas, leurs renseignements personnels ont été confiés à des gardiens des données qui n'ont peut-être pas de bonnes mesures de protection.

Par exemple, la FEC, le FBI et des sources canadiennes ont avancé qu'il faut au moins 6 mois et 200 heures — et selon des estimations que j'ai vues, cela peut aller jusqu'à 800 heures — pour redresser la situation une fois qu'il y a eu une atteinte. Dans bien des cas, cela arrive à des gens qui n'ont pas le temps ni les ressources qu'il faut pour régler ce type de situations. C'est un type de crime très malheureux qui évolue et dont sont victimes non seulement les personnes les plus indépendantes de la société, mais aussi les plus vulnérables.

Je voulais expliquer entre autres la différence entre les atteintes à la sécurité des renseignements personnels, les types d'information qui sont perdus lorsqu'il y a une atteinte à la sécurité dont nous entendons parler dans les nouvelles, le vol d'identité et, bien entendu, la fraude d'identité. Je pense qu'il est important de définir ces concepts ou du moins de ne pas les traiter de la même façon.

● (1545)

Je ne ferai pas un *Webster's* de moi-même aujourd'hui, mais je veux seulement m'assurer que nous faisons la distinction, car à mesure que la situation évolue et que de nouvelles tendances apparaissent, ces choses incluent des comportements très précis que nous pouvons et devrions suivre. En fait, pour prédire la façon dont elles évolueront, c'est important de le faire.

Nous voyons une explosion du piratage psychologique. L'hameçonnage — et l'hameçonnage ciblé — est l'une des pratiques les plus utilisées pour s'en prendre à des organisations, accéder à des ordinateurs personnels, installer des logiciels sans autorisation, etc. Si cette pratique est particulièrement efficace et nuisible, c'est qu'elle consiste à utiliser tout type de renseignements qu'on peut obtenir des victimes.

L'information ciblée a beaucoup à voir avec le taux de clics publicitaires et le nombre de courriels qui sont ouverts résultant de la réception d'un courriel ciblé. Par exemple, si je reçois un courriel ciblé de la CIBC contenant mon nom qui m'informe qu'il y a un problème concernant mon compte, il est fort possible que je clique dessus, surtout si je ne suis pas bien au courant des pratiques de sécurité à suivre.

Surtout, les pratiques que suivent les organismes canadiens ne sont pas uniformes lorsqu'il s'agit d'inclure des liens actifs vers des sites Web dans les courriels auxquels ils ont recours pour communiquer avec le public. Dans bien des cas, ces organismes devraient être plus avisés, et nous écrivons souvent sur le sujet.

Nous voyons bien que la menace est en partie attribuable à la quasi-légitimité des organisations qui induisent les gens en erreur, comme celles qui font apparaître une fenêtre intruse sur un écran indiquant que l'ordinateur a été infecté par un virus. Bien entendu, ce sont elles qui ont contaminé l'ordinateur et qui prétendent qu'il a été contaminé, mais en plus, il y a un prix à payer pour décontaminer l'ordinateur. Cette décontamination ne se fait qu'en partie.

Ce n'est peut-être pas en mettant toutes ces organisations dans le même panier, en les considérant toutes comme des entreprises criminelles, que nous arriverons à les attraper, car il sera très difficile de les poursuivre si, en fait, elles fournissent un service soi-disant légitime. C'est très difficile à faire, car nous avons constaté que dans bon nombre de cas, même si ces organisations n'infectent pas l'ordinateur ou n'utilisent pas de logiciel espion ou de choses qui se trouvent à être des pratiques publicitaires normales dans certains cas, dans bien des cas, ces gens ont même des services de soutien, et ils font des remboursements sans poser de questions. Il est très difficile d'adopter des mesures législatives qui empêcheraient ces personnes d'obtenir des renseignements personnels, d'en faire un usage abusif, de les revendre et de participer au cycle de cybercriminalité.

Nous savons qu'une bonne partie de ce type de ciblage de victimes inclut des appels téléphoniques, et non pas uniquement l'envoi de courriels. C'est très difficile pour les gens qui reçoivent l'appel de refuser. Dans bien des cas, on fait pression sur eux, et on les appelle à maintes reprises en utilisant des renseignements précis. J'ai moi-même reçu des appels de personnes qui m'ont demandé mes numéros d'assurance sociale et de permis de conduire, et elles étaient très insistantes. C'est très difficile pour les gens de savoir que ce type de choses se produit, et c'est difficile d'appliquer une politique visant à ne pas communiquer une partie de ces renseignements personnels.

Ce qui nous préoccupe, c'est ce qui se passe à l'échelle mondiale. Nous constatons que le vol de données est très répandu dans le monde, et je parle ici de vol de renseignements personnels. Il y a des liens avec certaines activités comme la traite de personnes et le financement du terrorisme. Nous ne sommes pas en mesure de fournir des chiffres précis à cet égard, tout comme c'est le cas pour la cybercriminalité, mais nous pouvons savoir où va l'argent.

● (1550)

Avec plus de collaboration de la police, particulièrement comme cela se fait en Europe, nous... Europol, par exemple, et Interpol obtiennent sectoriellement un succès énorme.

Nous constatons aussi l'utilisation inefficace des services de courtage de crédit, en réaction primaire aux atteintes. L'organisation victime d'une atteinte majeure offre immédiatement à toutes les victimes du crédit ne portant pas intérêt et la surveillance de leur identité. Ça s'arrête là. D'après nous, c'est insuffisant. Souvent, ses propres pratiques ne se conforment pas aux pratiques exemplaires normales de protection de l'identité ou de protection contre l'hameçonnage. La création de certains des outils qu'elle offre n'emploie pas de pratiques sûres. Dans la pratique, les contrôles sont très faibles, et il faudrait revoir la normalisation de ces sauvegardes.

De toute évidence, nous avons besoin de règles contre les pratiques prédatrices. Comme je l'ai dit, les organisations ne devraient pas être autorisées à victimiser des particuliers et à les appeler à répétition ni, c'est sûr, à les amener par la ruse à recevoir des services pour lesquels elles sont prêtes à des remboursements, parce que ce n'est pas ainsi que fonctionnent leurs modèles de gestion. Ces modèles fonctionnent grâce aux renseignements personnels qu'elles dérobent, et elles en tirent un profit facile. Elles vendent effectivement les renseignements de la victime et des détails personnels sur elle. C'est donc très important.

Il faut sévir plus rigoureusement contre la complicité dans la cyberfraude, mais nous devons aussi pouvoir déterminer l'intention coupable, par exemple, des nombreux individus qui cèdent aux promesses de profits sans, en fait, faire partie de l'élément criminel organisé. Souvent, ils voient une occasion de s'enrichir dans un emploi qu'ils croient honnête, puis ils se retrouvent en prison. On y voit un problème.

En guise de conclusion, il faut que tous sachent de la même manière à quel moment il est acceptable de communiquer son numéro d'assurance sociale, son numéro de permis de conduire et les risques qui en découlent, et, bien sûr, il faut agir sérieusement non seulement quand il s'agit de protection de la vie privée, mais aussi de données massives. Nous allons cerner des notions comme le vol et la fraude d'identité synthétique par l'analyse des données massives. Nous allons exiger la collaboration des banques et des sociétés d'assurance pour pouvoir reconnaître les tendances du risque et construire des modèles permettant de trouver les responsables. Actuellement, des individus, au Canada comme à l'étranger, gèrent quotidiennement en toute liberté des dizaines sinon des centaines d'identités non seulement de personnes existantes mais, aussi, de personnes fictives. Voilà aussi pourquoi les bureaux de crédit ne parviennent pas à les arrêter, et beaucoup de ces identités synthétiques continuent de porter préjudice à l'identité des victimes dont elles peuvent n'avoir emprunté qu'un seul élément d'identification pour le combiner à des éléments provenant d'autres individus et ainsi former un individu fictif dont les criminels se servent pour en retirer, pour eux-mêmes, des gains économiques ou financiers rapides.

Voilà ce que j'avais à dire. Merci de m'avoir donné l'occasion de vous en faire part.

● (1555)

[*Français*]

Le président: Je vous remercie.

Je vous arrête car votre temps de parole est un peu dépassé et pour permettre aux membres du comité qui sont ici aujourd'hui de vous poser des questions.

Passons tout de suite à une première ronde de sept minutes. Je rappelle aux membres du comité de mentionner à qui la question est adressée avant de la poser. Comme cela, les personnes qui sont en téléconférence et en vidéoconférence auront plus de facilité à savoir si la question leur est adressée ou non.

Je cède d'abord la parole à Mme Borg, pour sept minutes.

Mme Charmaine Borg (Terrebonne—Blainville, NPD): Bonjour.

Tout d'abord, j'aimerais remercier nos deux témoins. Les deux présentations étaient fort intéressantes.

Monsieur Popa, ma première question s'adresse à vous. Votre organisation n'est pas basée au Canada. Je suis particulièrement intéressée par le fait que votre organisation est internationale.

Où se situent les organisations canadiennes en ce qui concerne la protection des renseignements personnels? Y a-t-il des améliorations à apporter? Le Canada est-il un leader en la matière? D'après ce que vous avez observé, où le Canada se situe-t-il sur le plan international?

[*Traduction*]

M. Claudiu Popa: Il se trouve que je suis en vacances en Floride. Je vis et je travaille à Toronto; cependant, je suis en mesure de répondre à cette question. C'est la raison pour laquelle je ne vous ai pas interrompue.

[*Français*]

Mme Charmaine Borg: Je suis désolée.

[*Traduction*]

M. Claudiu Popa: Mon travail consiste à surveiller l'efficacité des lois contre la cybercriminalité mondiale. Comme nous conseillons les conseils d'administration, nous avons besoin de cette visibilité transectorielle et transnationale.

Nous constatons que les rumeurs disent vrai: la plupart des lois canadiennes et australiennes sur la protection de la vie privée sont intrinsèquement très innovantes et très efficaces, mais on ne les utilise pas efficacement. Nous trouvons que les organisations, dans leur ensemble — pas celles qui sont chargées de l'application de la loi, mais les entreprises — n'adoptent pas et n'appliquent pas à l'interne les bonnes pratiques pour au moins deux principes de la protection de la vie privée ou, du moins, des pratiques équitables de traitement de l'information. Il s'agit de la collecte et de la protection de l'information. Un troisième concernerait l'élimination de l'information. Il est très malmené. À l'étranger, c'est mieux.

Aux États-Unis, la loi est souvent bien appliquée en raison des sanctions financières rigoureuses, qui relèvent des lois sur la sécurité. Cependant, au Canada, qui ne possède pas beaucoup de lois sur la sécurité, l'application correcte des lois sur la protection de la vie privée pourrait profiter au public et le protéger contre la fraude d'identité, simplement par l'application de ces trois principes des pratiques équitables de traitement de l'information.

J'ignore si j'ai bien répondu à votre question, mais c'est ce que nous constatons.

● (1600)

[*Français*]

Mme Charmaine Borg: Merci beaucoup. Cela répond très bien à ma question.

J'aimerais m'excuser de vous avoir pris pour un Américain alors que vous êtes en vacances là-bas. D'ailleurs, nous sommes très jaloux de votre séjour au chaud.

Ma deuxième question est la suivante. Corrigez-moi si je n'ai pas bien compris votre allocution.

Vous avez dit que, lorsqu'il y a atteinte à la vie privée au sein d'une organisation, cette dernière répond souvent qu'elle va faire un suivi du dossier de crédit en cause. Vous avez semblé dire que ce n'était pas suffisant. Si c'est le cas, que proposez-vous? Comment devrait-on réagir lorsqu'une atteinte à des données pourrait mener à un vol d'identité?

[*Traduction*]

M. Claudiu Popa: Excellente question.

Nous constatons que notre recherche la plus significative se fait au niveau de l'entreprise, qui représente l'immense majorité des atteintes touchant les renseignements personnels, des atteintes qui font des dizaines ou même des centaines de millions de victimes. Les méthodes des grandes organisations pour répondre aux atteintes touchant les données nous apparaissent entièrement insuffisantes, parce qu'elles font intervenir une grosse machine. Dès le moment de l'atteinte, un puissant mécanisme intervient pour la sécurité des communications, qui a tout à voir avec la protection de la réputation. C'est la raison de son intervention immédiate. De toute évidence, il y aura collaboration avec la police, mais cela ne se fait pas assez vite.

Par exemple, le droit canadien sur la protection de la vie privée prévoit qu'il faut toujours une maîtrise immédiate de la situation et communication immédiate et écrite de l'information. Nous constatons que les entreprises prennent parfois un ou deux mois pour déclarer les atteintes. Bien sûr, les renseignements qui appartiennent aux victimes ont alors déjà amplement eu le temps d'être copiés, recopiés, revendus et reconditionnés de nombreuses fois. C'est un problème énorme.

Mais le gros problème est l'insuffisance de cette réponse, qui consiste simplement à s'informer auprès des bureaux de crédit sur les coûts par enregistrement. Combien coûtera la perte de 10 millions d'enregistrements? Avec le concours de TransUnion ou d'Equifax, elles offrent gratuitement, pendant une année, un service donnant aux victimes simplement accès à un tableau de bord et prévoyant l'envoi d'un courriel quand une atteinte du système est décelée. Je n'ai jamais rencontré quelqu'un qui ait reçu un message significatif concernant les données sur son identité. J'en ai rencontré quelques-uns qui en ont reçu sur la modification de leur cote de crédit, mais, par la suite, l'aide est minime. D'après nous, cette réponse est plutôt complètement insuffisante.

Pour la rendre suffisante, il faut d'abord que la loi fixe un délai d'un certain nombre de jours pour que les organisations contactent la police. Nous, nous préférerions qu'elles aient déjà mis au moins les commissaires à la protection de la vie privée dans le coup et qu'elles aient en place les bonnes pratiques et qu'elles aient fait faire les bonnes évaluations des répercussions sur la vie privée pour qu e la police et les commissaires puissent immédiatement les examiner et les analyser dès que l'atteinte a été décelée.

Au Canada, l'absence de notification des atteintes pose un inconvénient majeur, du moins à l'étranger, par rapport, disons, aux États-Unis, où cette notification est prévue par la loi. Ici, au Canada, ça n'existe pas, sauf dans certains secteurs comme les soins de santé dans l'ouest du Canada, mais ce n'est pas général. La notion est donc mal comprise et elle a été plutôt repoussée dans l'ombre, simplement parce que dès qu'on parle de l'obligation de signaler les atteintes, cela signifie automatiquement que chaque organisation doit effectivement investir dans des contrôles qui permettront de les déceler. Sinon, elles n'ont pas nécessairement besoin de s'en responsabiliser, parce qu'elles peuvent prétendre l'ignorance. Mais dès qu'elles les décèlent, elles doivent réagir.

La principale solution que je propose est d'exiger, dans la loi, la notification des atteintes, ce qui protégera le public.

● (1605)

[*Français*]

Le président: Je vous remercie.

Le temps de parole de Mme Borg est écoulé.

Je cède la parole à Mme Davidson, pour sept minutes également.

[*Traduction*]

Mme Patricia Davidson (Sarnia—Lambton, PCC): Merci beaucoup pour vos deux exposés sur un sujet très intéressant. Nous avons entrepris cette étude il y a de nombreux mois, mais la technologie et la situation elle-même évoluent si rapidement que chaque témoignage nous apporte du neuf.

Ce qui m'amène à ma première question, que je destine à Mme Sherbanowski.

Pourriez-vous, s'il vous plaît, nous dire ce que vous considérez comme la définition du problème du vol d'identité au Canada et comment il a évolué, non pas en 10 ans — le temps manquerait pour en parler —, mais récemment?

Pendant que vous y êtes, quelles en sont les causes les plus probables? Peut-être pourriez-vous préciser dans quelle proportion il touche des supports matériels, courrier, cartes de crédit, passeports, ou dans quelle mesure il survient en ligne.

Mme Janet Sherbanowski: À la faveur de notre collaboration avec les consommateurs dans le groupe ABCs of Fraud, j'ai vu sur son évolution toute l'information qui a été préparée. Au début, il y a 10 ans, c'était de petits numéros très vaudevillesques sur un coup de téléphone à une femme âgée par un escroc qui se faisait passer pour son petit-fils, ce genre de choses.

Les escrocs se sont raffinés. Cela pose l'une des difficultés suivantes: qui faut-il protéger? Les personnes âgées les plus vulnérables, qui emploient encore beaucoup de documents matériels? Les personnes âgées qui, comme moi, utilisent des technologies plus évoluées, l'ordinateur, pour toutes les opérations bancaires, le courriel et tout le reste? Les jeunes, qui ont des téléphones cellulaires et qui textent à la vitesse de la lumière? Actuellement, notre identité évolue à cette vitesse, et, d'après moi, les personnes les plus vulnérables sont les enfants. Leur utilisation des technologies et leur goût des communications continuelles sont extrêmement dangereux.

Mon petit-fils de 12 ans m'a appelée pour acheter en ligne un produit d'une valeur de 3,24 $. Je me suis aperçue que, pour l'occasion, il avait fourni beaucoup de renseignements sur lui-même. Un jeune de 12 ans parvient beaucoup mieux à donner des renseignements qu'un vieux de 60 ans. Le niveau et l'évolution du phénomène dépendent du groupe d'âge en question. Je pense que, maintenant, les plus vulnérables sont les jeunes, tant en ce qui concerne l'identité sexuelle que l'utilisation de leurs visages sur des images à contenu sexuel.

L'identité de quelqu'un constitue désormais une vaste nébuleuse. Ce n'est pas seulement le numéro d'assurance sociale, le numéro d'identification personnelle ou le numéro de permis de conduire. Ce peut être quelque chose qui devient un caractère animé. Vous avez participé à un jeu et vous avez créé une identité. Dans le cyberespace, cette identité devient très réelle, vendable, traçable et exploitable. Ces objets identitaires vont des objets matériels, sur papier, qui s'utilise encore, au Bitcoin et aux technologies qui valent des milliards de dollars, en passant par les technologies de jeu très sophistiquées.

La question est difficile, mais je dirais qu'elle évolue en ce moment même. Comme je l'ai dit, le courrier de ce matin m'a conduite à un détaillant qui, visiblement, a monté un projet de recherche dont l'objet est d'exploiter des données sur les enfants. Sur le plan de l'identité, nous parlons actuellement de l'utilisation de nos renseignements et de leur valeur. Voici d'où viennent les milliards de dollars. Ce n'est pas seulement moi, Janet; c'est ce que je représente pour quelqu'un, ailleurs, qui peut utiliser ces renseignements pour créer un produit et peut-être renverser un gouvernement. C'est très sophistiqué.

● (1610)

Mme Patricia Davidson: Très intéressante l'information que vous nous avez communiquée sur l'application qui permet de suivre les activités de nos enfants, si je vous ai bien comprise. Qui l'autorise? Les parents ou les commissions scolaires? Qui y participe?

Mme Janet Sherbanowski: Dans ce cas particulier, et j'obtiens ces nouvelles applications sans cesse, ce serait l'école, parce que cela n'allume pas vraiment les voyants rouges sur les enfants dont on espionne les sauts, à moins de fréquenter un comité comme le vôtre, n'est-ce pas?

J'enverrai le lien au comité, parce que je pense que c'est une facette très intéressante de notre sujet. Au départ, cela considère le saut comme une activité et cela envisage de compter la participation de l'enfant à des exercices de saut. Cela permet aux commissions scolaires de peut-être monter un programme d'études fondé sur cela, avec le nom de l'enfant, son âge et son activité physique. Nous n'allons pas divulguer délibérément cette information à quelqu'un pour qu'il espionne nos enfants, mais, en s'y prenant indirectement, ces organisations pourront suivre ces données.

Comme je l'ai dit, je crains, d'un point de vue très... J'ai reçu cela littéralement une heure avant de venir ici. Je suis allée sur le site et j'ai examiné l'application. C'est un petit programme bien fait, mais je ne tiens pas nécessairement à ce que ces renseignements sur un jeune enfant servent dans 20 ans.

Mme Patricia Davidson: Non, et je pense que cela conduit...

Le président: Madame Davidson...

Mme Patricia Davidson: Une petite question seulement.

[*Français*]

Le président: Soyez brève, madame Davidson.

[*Traduction*]

Mme Patricia Davidson: Cela conduit à la question: combien savent s'il y a eu vol d'identité?

Mme Janet Sherbanowski: Je pense que peu le savent. C'est l'une des grandes difficultés que je constate. Ce n'est pas signalé.

Il est sûr qu'on ne confie pas à notre police les ressources voulues pour s'en occuper. Si on a prévu un service pour recevoir l'information — et je travaille, à ce sujet, avec l'unité des crimes financiers de la police de Toronto — c'est presque considéré comme un crime sans victime. Ce n'est pas aussi préoccupant qu'une agression, un meurtre, un vol, sur la voie publique ou pas.

Dans les statistiques, on semble dire partout que la criminalité a diminué. C'est que, maintenant, on ne porte plus d'argent sur soi; seulement des cartes de crédit ou de débit. La baisse de la criminalité est une illusion. Le nombre de crimes n'a pas diminué. On ne les signale pas tous.

Mme Patricia Davidson: Merci.

Merci, monsieur le président.

Le président: Merci beaucoup.

M. Simms a maintenant la parole, pendant sept minutes lui aussi.

M. Scott Simms (Bonavista—Gander—Grand Falls—Windsor, Lib.): Je remercie nos invités.

J'avais préparé mes questions, mais en écoutant Mme Davidson, ma curiosité a été piquée par un phénomène que je trouve intéressant — et ma première question s'adresse à Mme Sherbanowski — c'est que la sous-notification de ce type de crime est une chose, mais, dans une circonscription comme celle que je représente, où la proportion de personnes âgées est élevée, on constate des réticences pour le déclarer.

Comment réagir? Vous avez dit avoir travaillé avec des groupes du programme Nouveaux Horizons. Comment approchez-vous les personnes âgées pour les informer sur la nature de ce crime, la façon de le reconnaître et la nécessité de le signaler?

● (1615)

Mme Janet Sherbanowski: Nous recevons du programme fédéral Nouveaux Horizons pour les aînés 25 000 $ pour sensibiliser les personnes âgées à la fraude. Nous recevons un certain nombre d'invitations, que nous sommes maintenant incapables d'honorer, de groupes de personnes âgées, d'hôpitaux, de centres d'hébergement et de soins de longue durée ainsi que du forum des personnes âgées de la ville de Toronto pour distribuer de la documentation. Il y a notamment le document intitulé *Le petit livre noir de la fraude*, produit par le Bureau de la concurrence, que nous avons distribué en grand nombre. Malheureusement, on ne peut maintenant que se le procurer en ligne. C'est un document très exhaustif, à la portée des personnes âgées. Procurez-vous en quelques exemplaires. J'ai pu en obtenir 200 pour les distribuer à divers groupes, puis, j'ai commencé à le photocopier. C'est un excellent document.

Les personnes âgées n'ont pas la même... Vous avez raison: elles ne veulent pas signaler les crimes. L'une des escroqueries les plus importantes est celle qui amène la victime à s'amouracher de l'escroc. Elle comporte à la fois un aspect frauduleux et un aspect embarrassant, pour s'être laissé soutirer de l'argent.

Un aspect aussi intéresse le vol d'identité, parce que, très souvent, la victime s'amourache d'une identité volée. Par exemple, quelqu'un, en Indiana, se prétend lieutenant des Marines des États-Unis. Un membre de mon conseil d'administration a été l'une de ses victimes. L'escroc a fini par demander 8 000 $ pour venir au Canada. Avant que cela ait pu se faire, non seulement mon amie avait-elle mordu à l'hameçon et communiqué des photos et des renseignements personnels, y compris des détails financiers et ainsi de suite, mais ces renseignements et ces photos ont pu ensuite servir à escroquer une autre belle victime romantique. Cela se propage vraiment.

Vous avez raison: les personnes âgées ne tiennent pas à signaler ce genre de crime. Quand nous allons les aborder à ce sujet, elles voient que je suis parvenue à un âge avec lequel elles peuvent certainement s'identifier. La communication en personne fonctionne donc très bien avec elles.

M. Scott Simms: Avant de poursuivre, quel était le nom de votre ressource?

Mme Janet Sherbanowski: C'est *Le petit livre noir de la fraude*. Il est produit par le Bureau de la concurrence.

M. Scott Simms: J'aimerais en obtenir des exemplaires.

J'aimerais vous poser ma prochaine question, monsieur Popa. J'espère que j'ai bien prononcé votre nom. Dans le cas contraire, je m'excuse.

Monsieur, vous avez mentionné certaines méthodes qui ont bien fonctionné en Europe. Parliez-vous de la cyberfraude, du cybercrime ou d'une combinaison des deux? Pourriez-vous nous décrire certaines des méthodes utilisées en Europe? J'aimerais entendre parler de celles que nous n'utilisons pas ici.

M. Claudiu Popa: Certainement. Je vous remercie d'avoir posé la question.

Nous avons constaté qu'Europol, par exemple, est manifestement un organisme d'application de la loi, mais il entretient de très nombreux liens avec son équivalent asiatique. Il a également des points de contact au Canada. L'organisme utilise des méthodes différentes, par exemple en faisant la promotion de ses réussites. L'une de ses récentes réussites a été réalisée dans l'industrie du transport aérien, où il y avait énormément de fraudes liées au vol d'identité. Des gens se servaient de ces identités volées pour parcourir le monde en avion pour des millions de dollars en billets d'avion, mais surtout, cela favorisait les déplacements de ces inconnus aux intentions non divulguées partout dans le monde. L'organisme a abondamment fait la promotion de cette récente réussite, et ses représentants ont affirmé qu'ils consacraient la même énergie à toutes les autres industries qui ont le même problème. J'ai mentionné cette réussite parce qu'elle est manifestement liée à notre sujet d'intérêt.

Il est évident qu'ils utilisent beaucoup la communication. De plus, ils collaborent et échangent des renseignements de façon très efficace; ils ne se contentent donc pas d'affirmer qu'ils sont également préoccupés par certains types de crimes, mais ils échangent des renseignements relatifs au comportement et aux données transactionnelles des personnes soupçonnées. Ils le font à plusieurs niveaux. Par exemple, nous sommes surtout préoccupés par la fraude d'identité d'entreprise. Dans de nombreux cas, ce type de fraude est le point de départ de la chaîne d'abus de confiance qui mène au vol d'identité personnelle. Une grande partie de ces fraudes d'identité d'entreprise préoccupe évidemment les entreprises. Elles exécutent des programmes de sensibilisation qui veillent à ce que les intervenants comprennent bien les répercussions de ce type de fraude sur la réputation de leur entreprise, sur leurs finances, etc., et elles sont grandement appuyées à cet égard en Europe.

● (1620)

M. Scott Simms: Désolé, je ne voulais pas vous interrompre, mais j'aimerais poser une dernière question.

Je trouve cela intéressant, car je suis allé en Europe de l'Est il y a quelque temps, et maintenant, plusieurs pays ont adopté des pratiques en matière de données ouvertes à grande échelle, par exemple l'Estonie et la Lettonie. Cette tendance semble s'étendre aux pays nordiques et même plus loin. Je présume que l'Union européenne en fera beaucoup plus, et je suis donc un peu surpris en ce qui concerne la politique en matière de données ouvertes, car ils ont toujours recours à des pratiques exemplaires pour réduire la cyberfraude et le cybercrime.

M. Claudiu Popa: Oui.

Désolé, quelle était votre question?

M. Scott Simms: C'est cela, oui.

M. Claudiu Popa: En fait, je fais la différence entre les stratégies en matière de données ouvertes et les pratiques exemplaires en matière de données ouvertes. Nous constatons que certains pays appuient les activités liées aux données ouvertes, mais ces stratégies en matière de données ouvertes ne sont pas nécessairement efficaces. Par exemple, des pays publient des données dont ils n'ont tout simplement pas besoin. Ils font l'inventaire de leurs données et décident qu'ils n'ont pas vraiment besoin de certaines données, mais avant de les détruire, ils les publient en tant que données ouvertes et c'est très bon pour leur image. Toutefois, ce n'est pas nécessairement utile ou efficace. De nombreux pays européens soutiennent qu'il s'agit de données de transaction rendues anonymes qui servent à obtenir des renseignements à valeur ajoutée, et non à créer des applications vendues à 99 ¢ pour générer des profits. Elles aident plutôt les organismes d'application de la loi à cerner des tendances concrètes et à mesurer les taux auxquels les gens cliquent sur des choses dans des secteurs vulnérables précis. Ces données ont été partagées par des organismes, des associations, des conseils et des organismes de publicité, et c'est utile. J'encourage donc la définition de données ouvertes en général comparativement au partage efficace de données ouvertes.

Le président: Merci. Votre temps est écoulé, monsieur Simms.

La parole est maintenant à Mme O'Neill Gordon. Elle a sept minutes.

Mme Tilly O'Neill Gordon (Miramichi, PCC): J'aimerais remercier les témoins d'être ici. Ils nous ont certainement communiqué beaucoup de renseignements utiles, et des renseignements sur lesquels nous pourrons réfléchir dans le cadre de notre étude.

Pour poursuivre dans la même veine, j'aimerais poser une question à Mme Sherbanowski. Existe-t-il une brève liste des mesures de base qui pourrait être distribuée à mes électeurs afin de les aider à protéger leur identité? Serait-ce utile?

Mme Janet Sherbanowski: Je vous remercie d'avoir posé la question.

Il existe une brève liste, et la réponse facile, c'est que nous pouvons évidemment dire: « Faites ceci, ceci et cela ». La réponse longue, c'est que lorsqu'on a commencé à installer l'électricité dans les foyers, tout ce qui fonctionnait à l'électricité pouvait être branché, ce qui provoquait de nombreux incendies. Ensuite, on a inventé les techniques de mise à la terre, etc. Tous les appareils qui viennent de l'étranger doivent d'abord obtenir l'approbation de l'Association canadienne de normalisation. Je suis certaine que vous avez tous vu cette étiquette. L'Association canadienne de normalisation s'occupe également des normes ISO et des diverses normes pour un grand nombre de choses, y compris les renseignements et les normes que nous devrions établir pour les renseignements.

Je crois que c'est ce qu'il faudra faire. Si nous tenons vraiment à protéger notre société, étant donné que nous étudions ce sujet de manière plus approfondie, à l'image des électriciens qui ont étudié l'électricité pour protéger les gens, nous devrons mettre au point une évaluation du risque pour les choses qui entrent dans notre pays et qui réussissent à déjouer nos protections jusque dans nos maisons, nos chambres à coucher et nos portefeuilles.

Je pense que tous les commissaires à la protection de la vie privée du Canada se sont penchés sur la question de la confidentialité. L'élaboration de mesures de protection qui précisent les pratiques permises aux entreprises devra faire partie des mesures que nous prenons en tant que société. Je sais que les banques, les sociétés d'assurances, les sociétés de santé et tous les autres étudient la question, mais on se dit que cela coûtera beaucoup d'argent, etc.

Il faudra assumer ce coût pour faire des affaires au XXI^{e} siècle. Je crois que ce coût en vaut la peine.

● (1625)

Mme Tilly O'Neill Gordon: Oui, c'est un coût que nous devons assumer pour améliorer les choses.

Vous avez également mentionné la journée « Changez votre NIP. » Est-ce que c'est une réussite partout au Canada? Le taux de participation est-il élevé?

Mme Janet Sherbanowski: Cette initiative commence à prendre son envol.

J'ai une proclamation le 20 mars. C'est le jour de mon anniversaire de naissance — et c'est également le premier jour du printemps — et c'est donc un bon truc pour me le rappeler. C'est une initiative semblable à celle utilisée pour se souvenir de vérifier les alarmes d'incendie et les détecteurs de fumée. C'est un moyen de stimuler la mémoire. C'est un peu quétaine, mais cela commence à fonctionner. D'autres groupes de prévention du crime de partout au Canada et dans le reste de l'Ontario commencent à adopter cette initiative. Je vais la présenter par l'entremise du Bureau de la concurrence.

Nous avons diffusé un communiqué de presse. Chaque année, notre association organise un dîner auquel nous invitons de 50 à 100 personnes âgées. Nous invitons également les représentants du Bureau d'assurance du Canada et de la Banque du Canada pour parler d'argent et de fraude. Nous parlons de fraude et nous envoyons des communiqués aux divers groupes de personnes âgées.

Comme je l'ai dit, tout le monde utilise une chose facile à se rappeler, afin de ne pas avoir trop de NIP, mais l'ajout de l'année à la fin ou au début complique la tâche à une personne qui tente de le deviner en regardant par-dessus votre épaule. Il s'agit seulement de rappeler aux gens qu'ils doivent protéger leur identité.

Mme Tilly O'Neill Gordon: Oui, et c'est une pratique qui sera adoptée par les gens, comme celle utilisée aujourd'hui pour les détecteurs de fumée. C'est maintenant une pratique commune, et d'ici quelques années, cette autre pratique le sera également.

Mme Janet Sherbanowski: Je l'espère.

Mme Tilly O'Neill Gordon: Pendant que j'écoutais vos deux exposés aujourd'hui, je pensais à au moins deux électeurs qui ont eu le malheur d'être victimes d'une escroquerie dans le cadre de laquelle ils ont divulgué leur identité, car ils croyaient recevoir de l'aide et des avantages par l'entremise de leur ordinateur, qu'ils ne pouvaient pas utiliser. Il y avait des problèmes. Ils pensaient gagner sur toute la ligne. Lorsqu'on leur disait qu'ils recevraient une compensation pour avoir fourni ces renseignements, ils les fournissaient très rapidement, peu importe combien de fois leur famille, leurs voisins et leurs amis leur disaient de ne pas le faire. C'est tout simplement une escroquerie à laquelle ils se laissent prendre.

Quelles nouvelles idées pourraient être proposées par notre gouvernement pour régler ce problème, par exemple des formations ou des cours offerts aux personnes âgées? J'aime l'idée que vous avez présentée au sujet de formations offertes dans le cadre de Nouveaux Horizons pour les aînés. De plus, de nombreux jeunes d'aujourd'hui seront victimes d'escroqueries.

Que pouvons-nous faire? Pouvez-vous nous recommander des éléments particuliers de ce problème sur lesquels nous pourrions nous pencher dans le cadre de notre étude? Il s'agit certainement d'une étude importante et nous tentons vraiment d'améliorer les choses pour tout le monde.

Mme Janet Sherbanowski: La question s'adresse-t-elle à Janet?

Mme Tilly O'Neill Gordon: À vous deux, s'il me reste assez de temps.

Mme Janet Sherbanowski: D'accord.

Si vous me le permettez, je répondrai en premier. Nous avons fondé le Groupe de travail sur les médias sociaux avec le Service de police de Toronto. Nous avons obtenu la participation du Bureau d'assurance du Canada, de toutes les banques, de Bell Canada, de nombreux groupes et des conseils scolaires. Deux fois par année, nous organisons une conférence sur les fraudes à Toronto. Cette conférence est diffusée à la télévision de Rogers et elle est également diffusée sur le site Web du Service de police de Toronto.

La première conférence que nous avons organisée portait sur la collaboration avec les médias, c'est-à-dire que tous les médias y ont assisté et ont écouté les spécialistes. Cela a commencé l'an dernier; c'est donc une nouvelle initiative à Toronto. Nous travaillons avec PhoneBusters et CARP. L'initiative prend de l'ampleur; même le tuteur et curateur public y participe maintenant. Les fraudes en matière de santé et les vols d'identité se poursuivent. Il s'agit d'un processus de sensibilisation.

● (1630)

Le président: Merci, madame Gordon.

[*Français*]

On me dit que l'heure dont nous disposions avec nos témoins est terminée.

Je remercie infiniment Mme Sherbanowski du temps qu'elle nous a accordé aujourd'hui. Je remercie également M. Popa, qui était en Floride, et lui souhaite une bonne fin de vacances. L'expertise de nos témoins sur le sujet nous aidera certainement pour la suite de notre étude.

Sur ce, je suspends la réunion pendant quelques minutes.

[*Traduction*]

M. Claudiu Popa: De rien. Je vous remercie de nous avoir invités à comparaître.

Le président: Merci.

Je vais suspendre la séance pendant quelques minutes et nous pourrons nous réunir à huis clos pour les travaux du comité.

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