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 142 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 4 avril 2019

Président

M. Bob Zimmer

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

Le jeudi 4 avril 2019

● (1530)

[*Traduction*]

Le président (M. Bob Zimmer (Prince George—Peace River—Northern Rockies, PCC)): La séance est ouverte. Nous entamons la 142e séance du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. Conformément au sous-alinéa 108(3)h)(vii) du Règlement, nous reprenons notre étude sur la protection des données personnelles dans les services gouvernementaux numériques.

Nous accueillons comme témoins, au nom de l'Association des banquiers canadiens, Angelina Mason, avocate en chef et vice-présidente, et Marina Mandal, vice-présidente, Transformation et stratégie bancaires. Pour le compte de Symcor Inc., nous accueillons Della Shea, vice-présidente, Protection des renseignements personnels et gouvernance des données, et chef de la protection des renseignements personnels.

C'est à vous Marina. Vous avez 10 minutes.

Mme Marina Mandal (vice-présidente, Transformation et stratégie bancaires, Association des banquiers canadiens): Merci, monsieur le président. Bonjour. C'est toujours un plaisir de comparaître devant le Comité.

Je m'appelle Marina Mandal et je suis accompagnée aujourd'hui de Mme Angelina Mason, l'avocate en chef et vice-présidente de l'ABC. Avant de poursuivre ma déclaration préliminaire, je tiens à m'excuser à l'avance si ma voix baisse en cours de route. Je suis aux prises avec un rhume, une grippe ou quelque chose de ce genre.

La notion de gouvernement numérique, quand nous vivons déjà dans une société numérique, devrait être bien accueillie. C'est particulièrement vrai dans le domaine de l'identification, où l'une des tâches fondamentales du gouvernement consiste à déterminer qui nous sommes et ce à quoi nous avons droit. Malgré des progrès technologiques remarquables qui s'accélèrent chaque année, nous sommes toujours liés à un modèle analogique qui repose sur la présentation de documents imprimés pour prouver notre identité dans le cadre des multiples transactions quotidiennes que nous avons avec les services publics, les entreprises et les uns avec les autres. La bonne nouvelle, c'est qu'il existe une solution moderne à ce problème. Le secteur canadien des banques est idéalement placé pour favoriser un système d'identification numérique qui révolutionnera la façon dont nous utilisons les données personnelles pour interagir avec le monde.

Le système actuel comporte trois lacunes majeures.

Premièrement, il est désuet, surtout quand il dépend de documents imprimés, comme les permis de conduire et les factures de services publics. Ces documents peuvent être contrefaits ou volés, et utilisés frauduleusement. L'obligation d'effectuer des transactions en personne impose également un fardeau aux personnes vivant dans des collectivités éloignées et aux personnes à mobilité réduite, qui pourraient être forcées de parcourir de longues distances pour effectuer des transactions de base ou accéder à des services essentiels.

Deuxièmement, même aujourd'hui, les systèmes fondés sur la technologie sont maladroits. Il est facile de compromettre la séquence d'identification à deux facteurs qu'on utilise en ligne — quand vous entrez un nom d'utilisateur et un mot de passe. C'est aussi un casse-tête pour les utilisateurs, qui doivent se rappeler des dizaines d'identifiants pour se connecter.

Troisièmement, l'inefficacité des méthodes de vérification de l'identité freine la croissance économique. Cela ralentit les transactions, crée de l'incertitude et entraîne des erreurs coûteuses. Des pays du monde entier se rendent compte que cette situation est intenable et se lancent dans l'univers électronique pour explorer les avantages de la mise en oeuvre de systèmes d'identification numérique.

Quand les pièces d'identité sont numérisées, on peut vérifier son identité électroniquement à l'aide d'une combinaison de systèmes existants et d'outils biométriques plus récents, comme les empreintes digitales ou la reconnaissance faciale. Étant donné que les Canadiens sont de plus en plus nombreux à consulter les services et les entreprises en ligne et qu'ils se servent de plus en plus de téléphones mobiles, le Canada peut envisager de créer un solide système d'identité numérique qui lui soit propre. Deux événements récents ont donné un nouvel élan à cette tendance.

Premièrement, les mises à jour apportées en 2018 à la Loi sur les banques permettent expressément aux banques de fournir des services d'identification, de vérification et d'authentification qui vont au-delà de leurs propres besoins opérationnels. C'est la reconnaissance contemporaine de ce qui a toujours été vrai des banques, à savoir qu'elles connaissent leurs clients, qu'elles connaissent leur situation financière et qu'elles peuvent attester les deux. Les banques ont toujours écrit des lettres de présentation imprimées pour aider leurs clients à régler des questions personnelles ou commerciales dans des endroits éloignés. L'aval d'une banque inspirait confiance parmi les étrangers.

Deuxièmement, l'ABC a publié l'an dernier un livre blanc qui expose clairement la voie à suivre pour faire de l'identification numérique une réalité au Canada. Nous avons tenu compte des caractéristiques uniques de notre pays, des institutions les plus modernes et de la complexité de l'infrastructure pour élaborer un cadre de référence susceptible de fonctionner ici.

Nous sommes en faveur d'un modèle fédéré d'identification numérique, parce qu'il serait aligné sur la structure politique du Canada. Un modèle fédéré crée des liens entre les systèmes fédéral et provinciaux de gestion de l'identité. À l'heure actuelle, l'identité est éparpillée dans de nombreux systèmes isolés. Par exemple, le gouvernement fédéral a des renseignements sur l'assurance sociale et les passeports, mais ce sont les provinces qui s'occupent des cartes d'assurance-maladie et des permis de conduire.

La première étape de notre modèle prévoit le maintien de ces systèmes distincts, mais la liaison des éléments disparates de façon à ce que l'identité d'une personne puisse être authentifiée électroniquement au moyen d'une combinaison d'attributs. Il est plus sûr de vérifier instantanément l'identité d'une personne qui utilise plusieurs éléments de référence numériques que de se fier à un permis en plastique qui pourrait être contrefait. Comme ce réseau numérique est connecté tout en étant décentralisé, on réduit le risque d'atteinte à la sécurité du système grâce à l'élimination des types de données que les pirates ont tendance à cibler.

La deuxième étape consistera à exploiter le pouvoir du secteur privé. On pourra ainsi créer un système d'identification numérique sans les coûts et les risques associés à l'élaboration complète d'une infrastructure complexe. Les banques canadiennes exercent déjà leurs activités partout au pays et dans le monde. Nous avons de solides systèmes électroniques interconnectés auxquels les citoyens peuvent avoir accès à partir de succursales, de guichets automatiques, d'ordinateurs personnels et de téléphones portables. Ces réseaux fonctionnent 24 heures sur 24, toute l'année. Mieux encore, les banques sont déjà tenues de respecter des normes élevées en matière de collecte et de protection des renseignements personnels de leurs clients. La confidentialité des données et des renseignements personnels de leurs clients est au coeur de leurs activités. Les banques font l'objet d'une surveillance rigoureuse visant à garantir que ces données sont conservées et protégées minutieusement tout au long de chaque transaction bancaire.

● (1535)

La troisième étape de notre modèle fédéré suppose l'adoption d'une loi permettant aux entreprises et au gouvernement d'accepter l'identification numérique. Les banques doivent connaître leurs clients dans le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme au Canada. Il faut commencer par recueillir et tenir à jour des renseignements financiers sur les clients, sous réserve d'une réglementation stricte. Il est vrai qu'on a modifié certaines exigences de la réglementation anti-blanchiment d'argent et anti-financement du terrorisme en matière d'identification des clients pour permettre la vérification indirecte, mais les règles continuent de s'appuyer sur une identification au moyen de documents imprimés.

Notre secteur est prêt et disposé à collaborer avec le Conseil du Trésor, le ministère des Finances, ISDE et d'autres organismes pour envisager des moyens d'inclure les technologies de l'ère connectée.

Le gouvernement a déjà commencé à examiner d'autres façons de mettre à jour les transactions financières, et l'intelligence artificielle et les chaînes de blocs sont en train d'ouvrir de nouveaux horizons. Compte tenu de cette évolution, la demande d'identification numérique se fera de plus en plus urgente. Les banques sont prêtes à fournir énergie et ressources pour construire un modèle fédéré pour le Canada.

Merci de votre temps. Je me ferai un plaisir de répondre à vos questions.

Le président: Merci encore.

Passons maintenant à Mme Shea, de Symcor Incorporated. Vous avez 10 minutes.

Mme Della Shea (vice-présidente, Privacy & Data Governance et chef de la protection des renseignements personnels, Symcor inc.): Bonjour. Je tiens à vous remercier, monsieur le président, ainsi que les membres du Comité, de me donner l'occasion de vous parler aujourd'hui d'un sujet aussi important et de vous faire part de notre point de vue, au moment où le gouvernement cherche à savoir comment améliorer les services offerts aux Canadiens tout en protégeant leur vie privée et leur sécurité.

Je m'appelle Della Shea. Je suis chargée de la protection des renseignements personnels et de la gouvernance des données chez Symcor et je vous présente cet après-midi mes observations fondées sur une vingtaine d'années d'expérience à la tête de programmes de sécurité et de protection des renseignements personnels reconnus à l'échelle internationale.

Pour ceux d'entre vous qui ne connaissent peut-être pas Symcor, nous sommes l'un des principaux fournisseurs canadiens de services d'impartition de processus opérationnels au secteur des services financiers. Nous offrons un portefeuille diversifié de services traditionnels aussi bien que numériques, dont le traitement des paiements, la production de relevés, la gestion de documents et l'analyse de la fraude. Nous fournissons également des services à d'autres organisations dans les secteurs du commerce de détail, des services publics et des télécommunications et, plus récemment, à certains gouvernements. Nous avons près de 2 000 employés dans tout le Canada.

Vous avez demandé comment le gouvernement peut améliorer les services offerts aux Canadiens tout en protégeant leur vie privée et leur sécurité. Pour répondre à cette question, j'aimerais vous faire part de certaines idées et expériences découlant de notre travail d'intégration da protection des renseignements personnels et de la sécurité dans nos services à Symcor.

Je vais surtout parler des moyens d'instaurer et de conserver la confiance des clients et, plus particulièrement, de trois principes fondamentaux qui sous-tendent la confiance, à savoir premièrement, la protection de la vie privée dès la conception et la gérance des données, deuxièmement, le rôle de fournisseurs de services de confiance dans un écosystème numérique, et, troisièmement, un cadre législatif cohérent. Je les aborderai l'un après l'autre.

Premièrement, comme beaucoup d'entre vous et de spécialistes de la protection de la vie privée le savent, la notion de protection intégrée dès la conception suppose que l'on tienne compte de la protection de la vie privée tout au long du processus de planification et de prestation des services. Autrement dit, la protection des renseignements personnels doit être le mode de fonctionnement par défaut d'une organisation. Les organismes gouvernementaux devront adopter une approche semblable. Je recommande de créer des mécanismes de contrôle applicables à la façon dont les gouvernements conçoivent leurs systèmes. Le cadre de protection intégrée de la vie privée devrait servir à intégrer la protection de la vie privée dans les activités opérationnelles.

La gérance des données est une deuxième notion étroitement liée à la protection intégrée de la vie privée. La gérance des données et son efficacité passent par une opérationnalisation du modèle de responsabilisation établi en vertu de la réglementation canadienne de la protection des renseignements personnels. Comme l'ont souligné les commissaires à la protection de la vie privée du Canada, il s'agit d'accepter clairement la responsabilité de la protection des renseignements personnels qu'ils contrôlent.

Puisque le gouvernement examine son mode de prestation de services aux Canadiens, je l'invite instamment à adopter un modèle de gérance des données. Très concrètement, il s'agit d'assumer la responsabilité de la protection de la vie privée et de la sécurité des Canadiens.

Je voudrais aussi aborder brièvement le rôle essentiel de fournisseurs de services de confiance dans l'écosystème numérique. Le virage vers les plates-formes et les écosystèmes est déjà en cours. C'est l'avenir de toutes les organisations et notamment des gouvernements. Le nouvel écosystème numérique permet de créer d'autres modèles opérationnels novateurs et de travailler avec de nouveaux partenaires, intermédiaires et collaborateurs.

En vertu de la réglementation canadienne de la protection des renseignements personnels dans le secteur privé, il existe une règle simple et efficace selon laquelle les organisations sont responsables des renseignements personnels dont elles ont la garde et le contrôle, y compris lorsque ces renseignements sont également transférés à des tiers.

Il est essentiel que le gouvernement mette en place un modèle de travail prévoyant des fournisseurs de services et des intermédiaires de confiance dans cet écosystème numérique. Selon ce modèle, les organisations seront tenues de respecter une norme uniforme afin de réduire le plus possible la probabilité de vulnérabilités systémiques, mais, de façon plus générale, afin de susciter la confiance dans l'écosystème numérique et la prestation de services numériques.

Dans le même ordre d'idées, pour gagner et conserver la confiance de la population, il faut des règles cohérentes et solides en matière de protection des renseignements personnels pour les activités de traitement des données par le secteur privé et le secteur parapublic, afin d'éviter toute lacune dans la protection des renseignements personnels.

Bref, tous les intervenants du monde numérique, dans le secteur privé comme dans secteur public, doivent respecter des lois cohérentes et rigoureuses en matière de protection de la vie privée. Le rôle du gouvernement sera fondamental dans l'instauration de règles cohérentes et robustes en matière de protection des renseignements personnels applicables à l'écosystème numérique.

● (1540)

J'en viens à ma conclusion. La feuille de route de la stratégie en matière de données publiée l'automne dernier pour la fonction publique présente une vision globale et permettrait de surmonter le cloisonnement des procédures et d'exploiter l'atout précieux que sont les données. Je félicite le gouvernement d'avoir entrepris cette étude de la protection des renseignements personnels et de la sécurité.

Je l'invite à concevoir un modèle de maturité qui s'adaptera progressivement, qui tient compte non seulement de la protection des renseignements personnels et de la sécurité au fondement même de la numérisation des services gouvernementaux, mais dont la perspective soit une société entièrement numérisée, où toute chose et tout le monde seront branchés sur un écosystème fluide et en expansion constante.

Merci. Je me ferai un plaisir de répondre à vos questions.

● (1545)

Le président: Merci, madame Shea.

Passons aux questions. Commençons par M. Saini. Vous avez sept minutes.

M. Raj Saini (Kitchener-Centre, Lib.): Bonjour. Merci beaucoup d'être parmi nous.

Madame Mandal, dans votre déclaration préliminaire, vous avez dit quelque chose que je voulais approfondir un peu, simplement pour mieux comprendre. Nous savons que, si nous voulons passer à un gouvernement numérique, nous avons besoin de la participation du secteur privé. Cela doit aller de pair si l'on veut tirer parti non seulement des renseignements confidentiels du secteur privé, mais aussi des technologies de pointe qu'il possède. Nous savons également que, de nos jours, l'information, surtout au Canada, est très décentralisée, que différents paliers de gouvernement détiennent de l'information, et même que différents ministères détiennent des renseignements différents.

Dans votre livre blanc, vous avez parlé d'un cadre fédéré d'identification numérique. Vous en avez parlé un peu dans votre déclaration préliminaire. Pouvez-vous nous donner une meilleure idée de la façon dont cela fonctionnera par rapport au modèle estonien X-Road? Vous avez dit quelque chose qui, à mon avis, fait penser à X-Road, à savoir qu'il n'y a pas de pots de miel. Mais, dans le cas de X-Road, ils sont partis de zéro. Ce n'est pas notre cas. Nos systèmes ont déjà plus de maturité. Et différents ministères ont des systèmes différents.

Comment peut-on comparer les deux? Comment le modèle fédéré fonctionnerait-il comparativement à X-Road, qui est un modèle différent appliqué en Estonie?

Mme Marina Mandal: Je vous remercie de votre question.

Je sais que le livre blanc de l'ABC, pour ceux d'entre vous qui ont eu l'occasion de l'examiner, parle notamment de deux pays, l'Estonie et l'Inde, qui sont très différents du Canada pour un certain nombre de raisons. Nous avons pensé, tout comme le Comité, je crois, que l'Estonie est en quelque sorte un modèle compte tenu de son contexte et de sa culture. Je dirais que les similitudes entre les leçons tirées de l'expérience de l'Estonie pour le Canada sont l'importance primordiale de la protection de la vie privée et de la sécurité des données. Je crois savoir que le projet d'échange numérique du gouvernement fédéral s'appuie sur une technologie semblable à celle qui sous-tend X-Road. Ce sont deux exemples que nous pouvons tirer de l'Estonie.

Mais, après cela, tout est très différent. Le modèle fédéré fonctionne selon le mode de gouvernance du Canada. Nous avons plusieurs paliers de gouvernement. Une identité de base sert à étayer différents niveaux. Les certificats de naissance relèvent des gouvernements provinciaux. Les documents relatifs à la citoyenneté et à l'immigration relèvent du gouvernement fédéral. Le modèle fédéré suit la logique de cette décentralisation. Je pense que la participation du secteur privé... Je pense qu'en Estonie, le gouvernement a adopté un modèle descendant, comme en Inde, alors que, au Canada, il y a déjà un mouvement. Nous avons des projets en cours. Je vais probablement reparler de deux ou trois autres choses dans mes observations d'aujourd'hui.

Le Digital ID & Authentication Council of Canada a été créé par le groupe de travail sur les paiements, nommé par l'ancien ministre des Finances M. Flaherty, parce que le groupe avait déclaré qu'il fallait absolument une identité numérique pour que les paiements numériques fonctionnent. Les gouvernements provinciaux, le gouvernement fédéral, les sociétés de télécommunications, les banques et les coopératives de crédit sont représentés au DIACC. Ils se sont regroupés pour créer un cadre de confiance pancanadien susceptible, dans l'idéal, de constituer une base pour tous les intervenants de l'écosystème numérique au Canada.

M. Raj Saini: Merci.

Madame Shea, j'aimerais revenir à vous. Je sais que vous connaissez bien le secteur privé.

Nous parlons d'un processus dit de socialisation organisationnelle. Pourriez-vous m'expliquer rapidement comment fonctionne ce processus au Canada? Cela toucherait 37 millions de personnes. Il y a des gens qui vivent partout au pays. Certains ont accès à Internet. D'autres, malheureusement, vivent dans des régions où il n'y a pas encore de service à large bande. Il y a des gens qui sont férus de numérique et d'autres, peut-être pas.

Comment faire pour que tout le monde embarque? Il faudra évidemment réaliser des économies d'échelle, et, pour que ce système fonctionne, tout le monde devra y participer. Le processus de socialisation organisationnelle me semble être l'une des grandes étapes limitatives, comme on dit en science. Comment cela fonctionnerait-il?

● (1550)

Mme Della Shea: J'aimerais faire quelques suggestions.

Dans mes commentaires, j'ai proposé l'adoption d'un modèle de maturité et expliqué qu'on ne peut pas tout faire en même temps. Il faut donc faire preuve de patience concernant la façon dont vous allez atteindre votre objectif de mise en place d'un service numérique, d'un gouvernement numérique et, au bout du compte, d'une société numérique. C'est la route à parcourir. Il s'agit d'être patient et d'avoir un modèle de maturité prévoyant des mesures claires pour répondre aux besoins de citoyens de tous les milieux.

M. Geist, qui s'est adressé au Comité précédemment, a parlé de la question de l'accès universel. Je pense que c'est une question très importante, à laquelle il faut réfléchir et à laquelle il faut s'attaquer, surtout compte tenu des limites géographiques et des défis propres au Canada. L'accès universel et abordable sera un défi de taille pour le Canada.

Il faut aussi comprendre, même si l'accès est possible, tout le monde n'aura pas la capacité de participer aux services gouvernementaux. Il y a le volet éducatif, qui devient un élément très important du casse-tête.

Je recommande au gouvernement d'envisager une procédure parallèle de mise en place de la socialisation organisationnelle et d'être patient. C'est une démarche. Tout le monde ne sera pas sur un pied d'égalité dans ce nouvel écosystème.

M. Raj Saini: J'ai une question complémentaire. Je vais changer un peu de perspective. Je vais vous poser cette question, justement parce que je crois que l'organisation que vous représentez a beaucoup d'expérience en matière de cybercriminalité et de cyberfraude.

Nous savons que la cybercriminalité et la cyberfraude sont à 80 % le fait d'organisations criminelles. Nous vivons à une époque où il y a des acteurs étatiques et des acteurs non étatiques. Bien qu'il n'y ait pas de pots de miel et qu'il n'existe donc pas d'endroit où se trouverait toute l'information, nous allons quand même y être enclins.

Il faut dire, concernant la protection de la vie privée, qu'on a un système solide à l'échelle nationale, mais que, à l'échelle internationale, en cas d'attaque éventuelle, de cybercriminalité et peut-être d'attaque contre une partie du système susceptible de contenir plus de renseignements qu'une autre, on se demande comment se protéger. La raison pour laquelle je pose cette question, c'est qu'il y a maintenant beaucoup d'acteurs non étatiques qui ont énormément de ressources et qui sont très bien financés. Comment régler ce problème?

Mme Della Shea: J'aimerais souligner l'importance de la mise en commun de renseignements confidentiels. À mon avis, si le gouvernement procède à une transformation numérique, il y aura des cyberattaques. Il y aura des menaces. Cela va de soi, et il s'agit donc de veiller à l'intégration de la sécurité dans les systèmes dès le début et de ne pas la considérer comme un type de contrôle parmi d'autres, mais bien comme un ensemble de contrôles multiniveaux.

À Symcor, par exemple, notre stratégie consiste vraiment en un modèle multiniveaux en matière de sécurité, depuis les données proprement dites jusqu'à l'application, en passant par l'infrastructure et le réseau. Il faut vraiment un modèle multiniveaux.

Il faut aussi penser à l'importance de la mise en commun de renseignements confidentiels et d'un cadre. Du point de vue législatif et politique, il faudra réfléchir à la question pour permettre la mise en commun de données entre les entités pour devancer les délinquants susceptibles de s'attaquer au système.

M. Raj Saini: Merci beaucoup.

Le président: Merci, monsieur Saini.

C'est à vous, monsieur Kent. Vous avez sept minutes.

L'hon. Peter Kent (Thornhill, PCC): Merci, monsieur le président.

Merci à tous d'être venus aujourd'hui.

C'était intéressant à suivre, particulièrement au sujet de l'association bancaire, de l'intérêt exprimé et de la vision mise à l'essai, dont votre président M. Parmenter, a parlé dans un discours en janvier.

Dans votre déclaration préliminaire, madame Mandal, vous avez parlé de trois difficultés, à savoir la maladresse, le caractère obsolète et le frein à la croissance économique. Lequel de ces problèmes les banques commerciales ont-elles abordé en premier ou croyez-vous qu'il soit possible pour la fonction publique, par opposition au secteur privé, de régler tous ces problèmes en même temps?

Mme Marina Mandal: Sur le fond, je pense qu'il faut absolument que ce soit un partenariat public-privé au Canada. Comme je l'ai dit dans ma réponse précédente, le gouvernement possède les documents de base qui prouvent l'identité, et je ne vois donc pas de solutions autonomes, du moins aucune qui soit actuellement sur le marché.

SecureKey Service de concierge est l'une des solutions proposées par le secteur privé en partenariat avec les banques. Je sais que vous avez entendu des représentants de SecureKey il y a quelques semaines.

Pour répondre à votre question, je dirais que le produit de SecureKey répond à ces trois éléments, mais pas tant à la question de la croissance économique, tout simplement parce qu'il s'agit d'un cas d'utilisation limitée à l'heure actuelle. Il permet l'accès à plus de 80 services gouvernementaux. Il élimine les utilisateurs qui n'ont accès à l'ARC qu'une ou deux fois par an, mais qui peuvent avoir accès à leur banque en ligne toutes les semaines ou aux deux semaines. Cela élimine la prolifération des noms d'utilisateurs et des mots de passe. Il suffit de se rappeler celui qui permet d'ouvrir une session dans le compte.

Il y a ensuite le caractère obsolète. Je rappelle qu'il n'est plus nécessaire de faire le lien, matériellement, avec l'ARC et d'autres services gouvernementaux.

Concernant la croissance économique, l'identité numérique est un marché assez nouveau au Canada, du côté du secteur public comme du côté du secteur privé. À mesure que le marché se développera dans les deux secteurs, je pense que nous verrons davantage de cas d'utilisation qui tiennent compte de la croissance économique.

● (1555)

L'hon. Peter Kent: Au sujet du caractère obsolète, nous avons entendu, il y a quelques mois, un témoin qui suggérait d'utiliser quelque chose comme la carte NEXUS et de faire appel à tous les outils biométrie, comme c'est le cas actuellement pour la sécurité des transports.

Les banques commerciales ont-elles envisagé de remplacer l'ancienne norme d'identification par la biométrie?

Mme Marina Mandal: Je crois que la biométrie serait assez contestée, compte tenu des obstacles législatifs, du côté des échanges par courriel. À ma connaissance, les banques commerciales ne s'intéressent pas à l'identification et à l'authentification numériques fondées sur la biométrie, pas au Canada en tout cas, et même pas — quand j'y pense — à l'échelle mondiale.

L'exemple d'utilisation de la biométrie pour l'identification numérique qui me vient à l'esprit est le projet en cours d'élaboration en Ontario, à l'appui de l'initiative de la province en matière d'identification numérique, qui s'appelle Eid-Me, je crois. Il s'agit d'un partenariat avec une entreprise de technologie financière. Chacun aurait son identifiant sur son téléphone, pour les besoins du gouvernement de l'Ontario seulement. Il y aurait un mot de passe et des éléments biométrie, à savoir l'empreinte du pouce ou la reconnaissance faciale. Dans le monde et au Canada, je dirais que c'est le principal endroit où l'on essaie d'utiliser la biométrie plutôt que la démarche bancaire d'ouverture de session par nom d'utilisateur et mot de passe.

L'hon. Peter Kent: Madame Shea, du point de vue du secteur commercial, que pensez-vous de l'utilisation de quelque chose comme la carte NEXUS pour l'identification numérique sécurisée?

Mme Della Shea: Le secteur privé est dans une situation différente en raison des exigences législatives. À mon avis, pour envisager un dispositif biométrique comme le modèle NEXUS, il faudrait que ce soit vraiment d'un modèle fondé sur le consentement. Ce serait essentiel, parce qu'il serait très difficile d'exiger que tous les Canadiens fournissent des données biométriques.

L'hon. Peter Kent: Du point de vue de la sécurité des transports ce n'est pas un problème, parce que les avantages l'emportent sur les préoccupations éventuelles.

Mme Della Shea: C'est exact.

L'hon. Peter Kent: Est-ce qu'on ne pourrait pas susciter l'intérêt dans d'autres domaines?

Mme Della Shea: Effectivement, à condition de s'assurer qu'il y a ce paradigme risque-avantage et de donner le choix aux gens, dans la transparence.

Cela dit, si c'est une option et que les gens l'adoptent pour rendre leur vie plus pratique, cela vaudrait la peine d'examiner cette possibilité. Le plus important, cependant, c'est d'avoir un système de sécurité vraiment solide et une gouvernance pour l'appuyer...

L'hon. Peter Kent: ... laquelle supposerait une modification de la loi.

Mme Della Shea: Oui.

L'hon. Peter Kent: Comme nous l'avons vu dans la fonction publique avec le système de paie Phénix, un des problèmes, c'est que, quand des gouvernements s'adressent à un fournisseur, ce dernier propose un produit et l'acheteur, et si ce dernier décide d'éliminer certains éléments de sécurité recommandés, on constate le désastre que nous avons aujourd'hui. Nous constatons la même chose avec le Boeing 737 et les options en matière de sécurité, qui supposaient des frais supplémentaires, une formation supplémentaire, etc.

Comment régler ce problème dans les partenariats du secteur privé avec le gouvernement à tous les niveaux? Comment s'assurer que les décisions politiques du gouvernement ne nuisent pas à l'efficacité du système?

Mme Della Shea: Tout déprendra de l'analyse coûts-avantages. Premièrement, il faut comprendre que la sécurité absolue et parfaite n'existe pas. Pour obtenir une sécurité ne serait-ce que presque parfaite, il faut non seulement prévoir des coûts, mais aussi mesurer l'utilité d'un service. Il faut donc équilibrer les enjeux.

L'Inforoute Santé du Canada est un exemple dont j'invite le gouvernement à tenir compte pour ce qui est de l'instauration d'un processus permettant aux fournisseurs de proposer une solution pour les services de santé. Les fournisseurs qui obtiennent l'agrément par ce mécanisme font l'objet d'une surveillance et d'une gouvernance. C'est un modèle que le gouvernement pourrait envisager pour définir le mode d'agrément des fournisseurs de produits ou de services souhaitant participer aux services gouvernementaux.

Il serait absolument essentiel d'appliquer des normes minimales et de prévoir un processus d'évaluation des divers fournisseurs désireux de faire partie de cet écosystème, puis d'exercer une surveillance permanente. Pour revenir à votre exemple des avions, il s'agit vraiment d'exercer une surveillance. Ce n'est pas un souci ponctuel. Il ne s'agit plus seulement d'un projet, mais désormais d'un produit, d'un processus et d'un cadre de gouvernance. Il est vraiment essentiel que ce soit permanent.

● (1600)

L'hon. Peter Kent: Ne pas se précipiter pour mettre un programme en place avant qu'il soit prêt.

Mme Della Shea: Tout à fait.

L'hon. Peter Kent: Madame Mandal, qu'en pensez-vous?

Le président: Le temps est écoulé, mais si vous avez un bref...

L'hon. Peter Kent: Oh, je suis désolé. J'y reviendrai.

Le président: Très bien. J'essaie d'être aimable.

La parole est à vous pour sept minutes...

M. Charlie Angus (Timmins—Baie James, NPD): C'est un peu plus que cela. Est-ce que je ne vous dis pas toujours que vous êtes un bon président?

Je ne vais pas contester la présidence aujourd'hui.

Le président: Allez-y, monsieur Angus.

M. Charlie Angus: Merci, monsieur le président.

Merci de cet exposé.

Je m'occupe constamment de fraude dans mes bureaux. Au début, il fallait être très naïf pour tomber dans les arnaques de la fraude 419, mais elles sont de plus en plus sophistiquées. J'ai été extrêmement surpris de voir combien de personnes — en fait, beaucoup de gens n'en parlent probablement jamais — ont été victimes de ces escroqueries.

La seule façon dont il semble qu'on puisse les arrêter, c'est littéralement lorsque le caissier de la banque dit non. Ce sont des gens qui veulent transférer des fonds à des parents en prison quelque part, qui veulent transférer de l'argent à quelqu'un qu'ils veulent épouser mais qui n'existe pas, qui veulent transférer des fonds parce qu'ils ont peur que l'ARC les arrête — c'est de plus en plus sophistiqué.

C'est pour cela qu'ils ont du pouvoir. Si vous avez un élément d'information sur quelqu'un, vous êtes encore loin du compte; si vous en avez deux, vous commencez à être bon; si vous en avez trois, vous devenez diablement précis. Grâce à l'intelligence artificielle, grâce à la possibilité de recueillir des renseignements dans Internet, la fraude se multipliera. Dans le travail que je fais au bureau de mon député, il semble que, bien souvent, la seule chose qui y mette un terme, c'est le caissier de banque qui dit: « Je crois que vous êtes victime de fraude. »

Quels mécanismes y a-t-il dans ce domaine pour commencer à s'attaquer à la sophistication croissante des méthodes de ciblage employées par les fraudeurs?

Mme Angelina Mason (avocate en chef et vice-présidente, Affaires juridiques, Association des banquiers canadiens): À mon avis, l'éducation est un élément important. Nous sensibilisons et informons les consommateurs pour qu'ils connaissent les risques. Il faudrait aussi échanger de l'information pour trouver des moyens technologiques de bloquer certains types de communications.

Scott Jones, chargé du tout nouveau Centre canadien pour la cybersécurité, nous a parlé récemment, dans le cadre de notre sommet sur la cybersécurité, des moyens technologiques qui permettraient de bloquer ces types de communications. Il y faudrait des analyses approfondies et une certaine convergence de fonctionnement des systèmes employés dans notre secteur, mais nous sommes très désireux de participer à ce genre de discussions pour voir si nous pouvons prendre des mesures encore plus proactives pour répondre à ce souci.

M. Charlie Angus: L'an dernier, 90 000 clients de Simplii Financial et de BMO ont été victimes d'une violation des renseignements financiers personnels. Les clients ont déclaré avoir reçu des réponses contradictoires au sujet du moment et de la portée de cette violation, et c'est inquiétant. Cette violation est-elle d'un acteur externe malveillant? Quelle était la nature de la fraude?

Mme Angelina Mason: Je ne peux pas vous donner de détails. Ce que je peux dire, c'est que nous sommes des chefs de file en matière de cybersécurité. Nous avons un excellent bilan. C'était un incident rare, et je peux vous assurer que les banques ont pris des mesures pour que leurs clients soient protégés financièrement et leur offrir d'autres formes d'aide.

Nous poursuivons ce combat. Nous cherchons toujours des moyens de déceler ces infractions. C'est une affaire quotidienne. Nous trouvons constamment des moyens de contrecarrer les attaques. Nous continuons d'examiner la question du point de vue de l'échange d'information et de la compréhension des nouveaux types d'attaques qui pourraient se produire. Nous investissons massivement dans cet espace et nous continuons d'en faire une priorité.

● (1605)

M. Charlie Angus: Je dois avouer que je ne garde pas mon argent à la banque. Je fais affaire avec une caisse populaire, mais j'ai été victime de quelques cas de fraude, et je suis stupéfait quand on me contacte immédiatement et qu'on me dit qu'il s'est passé quelque chose sur ma carte. Ce degré de vitesse est très intéressant.

Est-ce que cela fait partie de la tendance à accroître la capacité technologique d'intervenir pour mettre fin à la fraude?

Mme Angelina Mason: Oui. Il y a différents niveaux. Il y a les mesures de cybersécurité, qui visent effectivement les gens qui essaient d'avoir accès à l'information dans nos systèmes. D'autres types de violations peuvent survenir qui ne sont pas vraiment liées à la cybersécurité. On a peut-être utilisé votre nom d'utilisateur et votre mot de passe ou votre carte parce que quelqu'un a découvert ces codes et votre NAS.

En plus de protéger le cyberespace, nous faisons toutes sortes de suivis pour détecter les activités inhabituelles, repérer les différents types de violations et y remédier immédiatement.

M. Charlie Angus: La RBC a été signalée — je crois que c'était dans le *New York Times* — parmi les problèmes d'application de Facebook. Grâce à cette application, la banque aurait eu un accès privilégié lui permettant de lire des messages privés sur Facebook. La RBC dit qu'elle n'avait jamais eu cet accès. Facebook dit que oui. Le commissaire à la protection de la vie privée fait enquête.

Est-ce que l'Association des banquiers canadiens se penche sur ces questions pour être en mesure de garantir aux clients qu'une banque n'a pas indûment accès à ce genre de renseignements personnels?

Mme Angelina Mason: Nous ne nous occupons pas de cela.

Mme Marina Mandal: Non.

M. Charlie Angus: Très bien.

Une partie de notre travail consiste à protéger le droit à la vie privée des citoyens et les données privées. Je crois que la CIBC et la RBC ont au moins indiqué dans leurs politiques sur la protection des renseignements personnels que les données peuvent être transférées, traitées ou stockées à l'extérieur du Canada. Cela soulève des questions, selon nous, du côté de la protection des données financières.

Avez-vous une politique pour veiller à ce que les données soient conservées au Canada, où, au moins, grâce à nos lois sur la protection des renseignements personnels et nos normes nationales, nous saurions que les renseignements personnels restent confidentiels?

Mme Angelina Mason: Le fait d'avoir des données à l'étranger est commun non seulement aux établissements financiers, mais à toute une série d'entreprises. Le commissaire à la protection de la vie privée a abordé cette question dans ses lignes directrices.

C'est tellement courant que les méthodes sont diverses. Tout d'abord, la réglementation fédérale de la protection des renseignements personnels exige que, si des données doivent être conservées à l'extérieur du Canada, elles doivent, par le biais de contrats et d'autres mesures, être protégées tout autant qu'elles le seraient au Canada. Il y a aussi l'obligation de mettre les consommateurs au courant.

M. Charlie Angus: Aux États-Unis, est-ce que ces données sont assujetties au Patriot Act?

Mme Angelina Mason: Si vous parlez de la possibilité que ces données soient consultées de façon légale, ce serait possible, mais il y faudrait bien sûr un mandat.

M. Charlie Angus: Oui, j'ai eu affaire à un certain nombre de citoyens nés aux États-Unis, et il y avait toute la question fiscale, qui suppose qu'ils paient des impôts. Il y avait des gens qui vivaient ici depuis 40 ou 50 ans et qui étaient inquiets. Est-ce qu'on les informe que leurs données peuvent être conservées aux États-Unis et qu'elles sont assujetties au Patriot Act lorsqu'ils ouvrent un compte?

Mme Angelina Mason: Oui, nous leur disons où les données pourraient se trouver à l'extérieur du Canada et nous en expliquons les conséquences.

M. Charlie Angus: Merci beaucoup.

Le président: Merci, monsieur Angus.

C'est à vous, monsieur Picard. Vous avez sept minutes.

M. Michel Picard (Montarville, Lib.): Merci.

Ma question a trois volets. Comment comprenez-vous les systèmes bancaires ouverts? Qu'en pensez-vous du point de vue de la sécurité? Est-ce que ce serait un modèle, s'il est bon, qui pourrait être appliqué au gouvernement?

Mme Marina Mandal: Comme vous le savez sans doute, le gouvernement a publié son premier document de consultation officiel sur les services bancaires ouverts en janvier. Nous avons présenté un mémoire, avec d'autres intervenants, en février. J'y reviendrai dans un instant.

Depuis l'échéance de février, nous avons eu des conversations. Je dirais qu'il est très tôt pour parler des services bancaires ouverts. Nous avons abordé les commentaires en réfléchissant aux risques qui se posent à notre avis. Ces préoccupations étaient conformes à celles que le gouvernement a circonscrites dans son document de consultation, à savoir la protection des consommateurs, la protection de la vie privée, la lutte contre criminalité financière et la stabilité financière. Nous nous sommes principalement intéressés aux trois premières et nous avons discuté de stratégies d'atténuation des risques éventuels, du point de vue de l'organisme de réglementation aussi bien que du point de vue des solutions prises en charge par le secteur privé.

C'est le cadre dans lequel nous avons inscrit notre réflexion sur les services bancaires ouverts. Nous n'en sommes qu'au tout début et nous continuons de discuter avec le gouvernement lorsqu'il nous demande de lui faire part de notre point de vue. Mais, effectivement, il est encore tôt et il reste encore beaucoup à faire.

● (1610)

M. Michel Picard: Le fait que...

Mme Della Shea: Excusez-moi, est-ce que je peux ajouter quelque chose?

M. Michel Picard: Je vous en prie. C'est vous l'experte. Pas moi.

Mme Della Shea: Symcor a également présenté un mémoire à cette demande de communications.

Nos recommandations se rapportaient à ce que j'ai décrit plus tôt cet après-midi, c'est-à-dire des recommandations concernant la protection de la vie privée et la sécurité dès la conception. De plus, nous avions un cadre pour évaluer tous les intervenants de cet écosystème et nous nous préoccupions des vulnérabilités, qui sont essentiellement les maillons les plus faibles, de sorte que nous avions un processus d'évaluation approprié pour veiller à ce que tous les membres de cet écosystème maintiennent au moins un niveau minimal de protection de la vie privée et de sécurité.

Essentiellement, ce que nous avons recommandé, c'est de veiller à ce que la protection de la vie privée et la sécurité soient vraiment au-dessus de tout — alors nous pensions à l'utilité, à la commodité des systèmes bancaires ouverts — et aussi au fait que la protection des Canadiens était vraiment primordiale.

Encore une fois, comme Marina l'a mentionné, je pense qu'il est encore tôt. C'est un mandat important que le gouvernement doit examiner, surtout compte tenu de l'évolution de la situation à l'échelle internationale. Je crois aussi que c'est une occasion d'examiner les normes internationales. Encore une fois, c'est peut-être un peu prendre son temps pour progresser plus rapidement, éventuellement.

M. Michel Picard: En fait, le système gérait, dédoublait les données partout, et le concept de système bancaire ouvert propose que nous n'ayons qu'un seul endroit où se trouvent les données, et l'échange d'information où les différentes données doivent être combinées et utilisées... Si vous avez un système unique où vous avez des données uniques — du moins des sources uniques —, la beauté apparente de ce système, c'est que vous ne regardez pas partout. C'est juste en un seul endroit. Vous avez besoin d'un système de sécurité très sophistiqué pour éviter une intrusion, parce que si vous êtes victime d'une intrusion, vous perdez tout. S'agit-il d'un risque calculé?

Mme Marina Mandal: Je pense que vous avez tout à fait raison de parler des principales préoccupations de l'Association des banquiers canadiens au sujet de la cybersécurité et de la criminalité financière en général dans le contexte des systèmes bancaires ouverts, où, comme vous le savez, le client consent à ce que ses renseignements personnels et financiers soient transférés à un autre fournisseur, qu'il s'agisse d'une banque ou peut-être d'une technologie financière qui n'est pas aussi rigoureusement réglementée que les banques.

Une fois que cela se produit, et si cette information se retrouve plus loin dans le processus, le fournisseur tiers la fournit à une autre partie, nous nous inquiétons à la fois de la connectivité accrue et de la prolifération des entités qui ont accès aux données. Cela rend certainement plus difficile, dans le cas d'une cyberattaque, de déterminer vos points de vulnérabilité, numéro un et numéro deux. Encore une fois, les fournisseurs tiers ne seront pas tous réglementés de la même façon.

Nous avons été heureux de voir dans le budget de cette année l'annonce prochaine de la loi sur la cybersécurité, mais nous nous inquiétons pour les entités qui pourraient ne pas faire l'objet d'une surveillance réglementaire complète tant pour la protection de la vie privée que pour la cybersécurité.

M. Michel Picard: Madame Shea, dans votre déclaration préliminaire, vous avez mentionné à maintes reprises le mot « fiable ». Quels sont les critères pour être un fournisseur fiable? En affaires, la confiance n'existe pas...

Mme Della Shea: Donc...

M. Michel Picard: ... et en politique, je suppose.

Mme Della Shea: Pour moi, le terme « fournisseur fiable » signifie vraiment que vous avez un engagement à l'égard de vos valeurs et de vos normes dès le départ, et que vous avez du soutien depuis le sommet de l'organisation et à chaque niveau.

Essentiellement, c'est nécessaire pour faire ce que vous promettez de faire. Il ne suffit pas d'avoir une déclaration ou une politique disant que vous allez protéger la vie privée. Il faut vraiment avoir l'infrastructure, la communication, l'adhésion de tous ceux qui participent à la prestation d'un service. Ils doivent comprendre, premièrement, quels sont leurs objectifs et leurs obligations et, deuxièmement, ils doivent savoir qu'ils ont les outils nécessaires pour les réaliser. Cela exige vraiment un engagement. Il faut une compréhension à l'échelle de l'organisation tout entière, et la compréhension revient vraiment à rendre les choses simples et faciles pour quiconque afin qu'il puisse comprendre ce qu'il doit faire pour obtenir cette confiance ou cet engagement. Dans ce cas-ci, nous parlons de protection de la vie privée, alors qu'est-ce que cela signifie? Cela veut dire de faire en sorte que tout le monde comprenne.

Chez Symcor, nous y sommes parvenus en mettant en œuvre un ensemble de valeurs de données. Nous avons un ensemble de valeurs de données qui militent en faveur de la protection des renseignements personnels, de la responsabilisation, de la conformité et de la confiance, et nous tirons parti de ces valeurs pour être en mesure de communiquer avec tout le monde. Il ne s'agit pas simplement d'un tas de choses enfouies dans une politique. Ce sont des choses que vous vous engagez à faire tous les jours. Cette communication est mise en œuvre au moyen de nombreuses activités intéressantes et amusantes. Nous organisons une journée annuelle de protection des données, où nous avons des jeux-questionnaires et des jeux. Nous avons de la formation. Nos données sont en fait représentées par une petite mascotte, qui est en fait un hibou. Il est très populaire dans l'ensemble de l'organisation. Les gens ont hâte de prendre connaissance de ses notes et de ses messages.

Il s'agit de faire ce que vous dites que vous allez faire, puis de le soutenir avec l'engagement, qu'il s'agisse d'un engagement financier, parce qu'il faut aussi ce niveau d'engagement...

● (1615)

M. Michel Picard: Merci.

Le président: Merci, monsieur Picard.

Le prochain intervenant, pour cinq minutes, est M. Gourde.

[*Français*]

M. Jacques Gourde (Lévis—Lotbinière, PCC): Merci, monsieur le président.

Je remercie les témoins d'être ici aujourd'hui.

Dans cet univers d'identification numérique, je pense que les Canadiens méritent et ont le droit de savoir que leurs données personnelles demeureront confidentielles. Je m'interroge avec inquiétude sur l'hébergement hors frontières des données numériques, ces dernières étant alors assujetties à des lois autres que celles du Canada.

Selon vous, devrions-nous privilégier l'hébergement de données numériques canadiennes au Canada pour simplifier la résolution de tout problème éventuel, ou pouvons-nous juger que les lois étrangères sont comparables et n'avoir aucune inquiétude?

[*Traduction*]

Mme Angelina Mason: Je vais demander à Mme Mandal de vous parler de la composante des données numériques, mais en ce qui concerne l'exigence de protéger l'information, comme je l'ai dit plus tôt, notre cadre de protection des renseignements personnels nous permet d'avoir des données au Canada et à l'étranger, à condition que nous ayons des mesures contractuelles et autres appropriées pour assurer le même niveau de sécurité.

Mme Marina Mandal: Pour ce qui est du lien entre les données et l'identité numérique, je veux m'assurer que nous comprenons bien. Je sais que vous avez entendu SecureKey, et j'utilise SecureKey comme exemple parce qu'il s'agit d'un partenariat entre le secteur privé et le secteur public qui est sur le marché.

L'authentification à triple insu dont ils ont parlé signifie que personne n'a vu les données. Disons que je vais à la banque, ou que j'utilise mes justificatifs bancaires pour ouvrir une session à l'ARC. La banque ne le sait pas; l'ARC ne sait pas qui est ma banque, et SecureKey ne voit rien de tout cela. Selon la technologie, personne ne voit quoi que ce soit. Tout se fait de telle façon que, évidemment, je choisis, je donne mon consentement ou j'utilise le produit de façon proactive. La carte d'identité numérique n'est pas un échange de données; ce n'est pas un système bancaire ouvert. Il s'agit simplement des composantes d'authentification et de validation des attributs.

[*Français*]

M. Jacques Gourde: Vous avez recommandé tout à l'heure de prendre le temps de mettre en place ces nouvelles technologies pour s'assurer qu'elles seront utiles et qu'elles fonctionneront bien. Selon vous, « prendre le temps » signifie-t-il de un à trois ans, de trois à cinq ans, ou plutôt dix ans?

[*Traduction*]

Mme Della Shea: Je veux simplement m'assurer de bien comprendre la question. Il s'agit de l'horizon temporel pour mettre en œuvre des technologies de façon sécuritaire.

Je crois qu'il s'agit d'un processus continu, alors je ne crois pas nécessairement qu'il y ait un élément temporel précis lié à cela. À l'heure actuelle, les technologies ne sont pas toutes sur un pied d'égalité. Certaines sont beaucoup plus matures que d'autres. Si vous regardez les grands joueurs qui ont investi beaucoup de temps, d'énergie et d'argent dans ces technologies, là où il y a une l'histoire, ce sont des choses qui pourraient être plus facilement adoptées.

Toutefois, à mesure que les nouvelles technologies arrivent sur le marché, je tiens à souligner qu'il nous faut un moyen efficace de procéder à une évaluation adéquate pour nous assurer que ces technologies atteignent l'objectif réel. Cela va au-delà de la protection de la vie privée et de la sécurité pour s'assurer que l'utilité et la fonctionnalité font ce qui était prévu à l'origine. Je crois qu'il n'y a pas de solution universelle. Il pourrait y avoir une approche à plusieurs niveaux pour évaluer les technologies établies sur le marché par rapport à celles qui émergent.

● (1620)

[*Français*]

M. Jacques Gourde: Pour en rendre l'évaluation plus efficace, devrait-on implanter ces nouvelles technologies de façon graduelle, en commençant par un secteur, une ville, une région ou une province du Canada, plutôt qu'à l'ensemble de la population, permettant ainsi d'éviter le genre de problèmes que l'on a connus dans le cas d'autres services?

[*Traduction*]

Mme Della Shea: C'est une excellente recommandation. En gros, si vous évaluez une fois, vous pouvez l'appliquer plusieurs fois, et c'est un facteur d'efficacité important. Comme je l'ai mentionné plus tôt, Inforoute Santé du Canada a une structure qui lui permet de certifier une technologie. Cela permet essentiellement à d'autres de tirer parti de cette technologie dans l'industrie des soins de santé sans avoir à faire la même évaluation encore et encore.

Mme Marina Mandal: Je peux ajouter quelque chose. Je suis tout à fait d'accord pour dire que c'est une excellente idée. C'est une façon de procéder à des essais itératifs sans compromettre les renseignements sur les clients. Pour signaler quelques endroits où cela se produit, au Nouveau-Brunswick, le gouvernement a mis en place des pièces d'identité numériques — je parle précisément de la technologie entourant l'identification numérique — uniquement dans le cadre d'un projet pilote. En Colombie-Britannique, je crois que c'est aussi l'intention.

L'Illinois utilise une carte d'identité numérique précisément pour déterminer qui est autorisé à être médecin, alors il y a ce genre de cas d'utilisation également. Les besoins sont peut-être très élevés là-bas pour une raison ou une autre. Il y a des cas d'utilisation fondés sur la technologie utilisée, ainsi que sur le type de problème d'authentification que vous essayez de résoudre.

[*Français*]

M. Jacques Gourde: Je vous remercie.

[*Traduction*]

Le président: Merci, monsieur Gourde.

Nous passons maintenant à M. Erskine-Smith, pour cinq minutes.

M. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Merci beaucoup.

J'ai quelques questions au sujet de l'identité numérique, mais ma première question porte davantage sur la protection de la vie privée.

Le 24 octobre, j'ai fait un achat au magasin Ontario Cannabis Store, et il a fallu des semaines pour que l'achat soit livré parce que le gouvernement conservateur provincial de l'Ontario ne peut même pas vendre de mari comme il faut. J'ai fini par recevoir mon achat et il a été inscrit sur mon relevé de carte de crédit. C'est très bien. Je suis citoyen canadien. Il est légal d'acheter du cannabis en ligne, comme cela doit se faire. Toutefois, ce n'est pas légal aux États-Unis, alors nous entendons parler de Canadiens qui traversent la frontière et à qui on demande s'ils ont consommé du cannabis au cours de leur vie, parce que cela demeure un crime dans la plupart des endroits aux États-Unis.

Quelle assurance ai-je, comme Canadien, que le relevé de carte de crédit qui reconnaît la transaction d'un achat licite au Canada, mais une activité illicite aux États-Unis, est protégé et que ma vie privée est protégée?

Mme Angelina Mason: À ce sujet, si vous parlez de l'endroit où se trouvent les données transactionnelles — disons, par exemple, qu'elles se trouvent aux États-Unis —, la seule façon d'accéder à ces données pour voir si vous répondez ou non à cette question serait de passer par un processus de mandat officiel en vertu de la Patriot Act.

Je ne pense pas que ce soit un problème réel. Je ne pense pas que ce serait appliqué de cette façon. Cette mesure législative vise vraiment à traiter des cas d'importance nationale, et non pas de la consommation d'une substance par une personne en particulier. Je ne crois pas que ce soit un problème.

M. Nathaniel Erskine-Smith: Les banques se sont-elles penchées sur la question, lorsque des Canadiens se livrent à des activités légales ici qui sont illégales dans des endroits où nous allons fréquemment, comme aux États-Unis, pour veiller à ce que les autorités américaines n'aient pas accès aux dossiers de ces activités de quelque façon que ce soit?

Mme Angelina Mason: À titre de précision, nous aurions des protections contractuelles pour nous assurer qu'elles ne sont pas communiquées, bien qu'il soit possible qu'un mandat en bonne et due forme soit signifié dans ce pays. Cependant, je ne peux pas m'attendre à ce qu'un mandat soit signifié dans ce contexte, parce que si c'était quelque chose d'aussi important que le Patriot Act, j'imagine que ce serait quelque chose de la nature d'un crime national, et non d'une consommation personnelle.

M. Nathaniel Erskine-Smith: Je suis moins inquiet, selon toute probabilité.

En ce qui concerne l'identification numérique, dans votre déclaration préliminaire, j'ai remarqué que vous êtes prêts à aider le gouvernement du Canada. Nous avons reçu Alex Benay, qui nous a parlé de l'identification numérique fédérée et des mesures qu'il a prises à cet égard. Du point de vue de l'Association des banquiers canadiens, quelles sont les prochaines étapes à suivre pour nous rapprocher de cette identité numérique fédérée?

● (1625)

Mme Marina Mandal: Ce qui est extrêmement important, c'est le travail effectué par le Digital Identification and Authentication Council of Canada sur le cadre de confiance pancanadien. Pour bon nombre des questions qui ont été posées jusqu'à maintenant par le Comité et des choses dont nous avons parlé — la protection de la vie privée, la sécurité des données, les normes qui transcendent les frontières, la transparence de la gouvernance, les normes ouvertes —, l'intention est de les régler et de les mettre en place par l'entremise du cadre de confiance pancanadien.

Pour ce qui est de l'échéancier, l'achèvement prévu du cadre de confiance est fixé à l'année prochaine. Il y a des projets de discussion qui sont en cours de production à l'heure actuelle aux fins de commentaires du public, alors ils sont ciblés pour 2020.

C'est une première étape cruciale. Les normes comprennent la protection de la vie privée dès la conception; il y a donc 10 principes sous-jacents à un écosystème d'identification numérique.

L'autre aspect positif du processus du cadre de confiance pancanadien du Digital Identification and Authentication Council of Canada, est qu'il y a différents ordres de gouvernement à la table, différents intervenants du secteur privé et des entreprises de technologie qui pourraient aider à trouver une solution du point de vue technologique. Cela crée l'interopérabilité.

En principe, le gouvernement fédéral est en train d'élaborer, ou a l'intention de le faire, avec, je crois, Connexion Canada, sa propre solution d'identification numérique, mais vous avez la solution d'identification numérique de SecureKey qui est également censée correspondre à ce à quoi ressemblera le cadre de confiance pancanadien. Cela permet au gouvernement fédéral, par exemple, ou à un gouvernement provincial, de dire que vous pouvez utiliser l'un ou l'autre. Si vous allez au Nouveau-Brunswick en ce moment, où l'on mène des projets pilotes sur l'identité numérique, vous pouvez vous connecter au projet pilote du Nouveau-Brunswick en entrant votre carte d'identité numérique émise par le gouvernement du Nouveau-Brunswick ou votre carte d'identité numérique SecureKey Service de Concierge.

À mon avis, c'est la prochaine étape. Un autre aspect plus vaste, dans le cadre duquel l'Association des banquiers canadiens joue un rôle, consiste simplement à socialiser le concept, pour s'assurer, comme l'un des députés vient de le dire, que les Canadiens se sentent en sécurité. Ils doivent comprendre le produit, car les Canadiens entendent constamment parler de cyberatteintes. C'est aussi le volet éducatif et promotionnel de l'identification numérique.

Le président: Merci, monsieur Erskine-Smith.

Le prochain intervenant est M. Kent, pour cinq minutes.

L'hon. Peter Kent: J'aimerais poursuivre sur ce point. L'un des défis au Canada, contrairement à l'Estonie, est le scepticisme du public à l'égard de la protection du dossier de santé et du dossier financier d'une personne. Cela concerne l'ARC, pas nécessairement les banques, même si, comme l'a dit M. Angus, la fraude est certainement un problème croissant et il y a toutes sortes de façons de le faire. Bien que les banques aient réussi à contrer cette pratique de façon très efficace, il m'est arrivé, à moi aussi, que la banque m'informe d'une tentative d'utilisation d'une carte et de son numéro dans les minutes qui ont suivi la tentative.

Le secteur privé recommanderait-il des projets pilotes sur une base plutôt limitée, voire semi-régionale, étant donné qu'il y a des générations de Canadiens qui n'utilisent pas vraiment les appareils numériques, même qu'ils continuent d'insister pour qu'il y ait un caissier humain à leur banque et que leurs transactions se fassent sur papier? Recommanderiez-vous un projet pilote réduit, assez étroit, contrairement au Nouveau-Brunswick, mais peut-être d'abord les centres urbains, d'une certaine façon?

En Ontario, par exemple, à Toronto, nous avons constaté l'incapacité de mettre en œuvre l'échange numérique de renseignements médicaux entre les omnipraticiens, les spécialistes, les hôpitaux, les cliniques, etc. Cela fait 20 ans qu'on en parle, et c'est encore un projet incomplet, imparfait. Proposeriez-vous des projets pilotes dans un domaine particulier? Cela pourrait être lié aux soins de santé ou à l'ARC, mais encore une fois, à une échelle très limitée, l'élaboration d'un modèle de réussite pourrait-elle donner confiance à des groupes démographiques plus réticents à adopter et à participer?

● (1630)

Mme Della Shea: Je crois qu'un projet pilote est logique sur le plan pratique pour un certain nombre de raisons. Le simple fait d'essayer d'amener des gens à participer, de communiquer et d'éduquer les gens sur ce que cela signifie serait intenable.

Pour ce qui est de la réalisation d'un projet pilote, cependant, je recommanderais que ce soit sur une base d'adhésion, dans le but d'élaborer quelque chose avec l'intention de le reformuler, afin de s'assurer que vous n'essayez pas de tout inclure et d'être parfait, mais que vous commencez tout simplement à participer.

Ce serait aussi une façon très pratique de commencer à introduire le concept, surtout s'il est établi de façon à ce qu'il s'agisse d'une activité facultative dans le cadre de laquelle les responsables de l'élaboration des solutions prendraient cette information. La participation du public serait un modèle intéressant, mais il serait certainement important de savoir et de comprendre qu'il s'agit d'un processus itératif.

Je crois que c'est vraiment l'objectif des principes de protection de la vie privée dès la conception. Il s'agit de comprendre les exigences dès le départ, puis, tout au long du processus, de vérifier si nous avons respecté ces exigences initiales et si nous avons respecté cette intention. Ensuite, il faut prendre cette rétroaction et l'itérer encore et encore.

Mme Marina Mandal: Merci.

Je tiens à souligner qu'en ce qui concerne le scepticisme du public, je suis tout à fait d'accord. Nous parlons beaucoup d'innovation ces jours-ci, certainement dans le secteur bancaire, et il est évident que votre comité s'est penché sur la transformation numérique dans le contexte gouvernemental. Il est essentiel pour la confiance des consommateurs de savoir que la sécurité des renseignements personnels sera assurée.

C'est notre point de départ. Comme je l'ai dit plus tôt, une partie de ce rôle consiste à éduquer le public, comme le font, je crois, le secteur public et le secteur privé. On explique aux gens que l'identité numérique n'est pas une entreprise dont vous venez d'entendre parler, SecureKey, qui transmet toutes vos données. Elle ne les voit pas vraiment, n'est-ce pas? Il est très utile de suivre ce processus d'explication en utilisant le langage le plus simple possible.

Ensuite, il faut se demander si les gens de l'écosystème respectent les normes et les principes. Est-ce que tout le monde s'entend là-dessus, et sont-ils assez élevés?

Il y a une différence entre une banque, une entreprise de télécommunications ou un gouvernement provincial ou fédéral qui authentifie votre identité en ligne et Facebook ou toute autre entreprise de médias sociaux, uniquement parce qu'il s'agit d'identités autocréées. Il n'y a pas d'identité fondamentale sous-jacente émise par le gouvernement.

Lorsque vous parlez d'identification numérique et d'analyse de l'appétit du public, ce sera aussi l'appétit du public seulement, en fonction des personnes que vous amenez dans l'écosystème, du genre de produits qu'elles offrent, ainsi que de l'optionalité et de la commodité pour le consommateur.

L'hon. Peter Kent: Dans le cas des projets parallèles du Nouveau-Brunswick, des deux approches, y a-t-il quelques premiers éléments qui puissent donner une idée du degré de satisfaction des utilisateurs?

Mme Marina Mandal: Je n'ai pas pu trouver beaucoup d'information à ce sujet. Ce semble être un projet pilote assez fermé. Il s'agit simplement de faire des tests bêta des deux côtés: la technologie du gouvernement du Nouveau-Brunswick et le SecureKey Service de Concierge, qui est en place depuis un certain temps.

Je suis désolée. Je n'ai pas tout à fait répondu à la question sur le projet pilote.

La question est intéressante. Mme Shea et moi-même vous avons parlé aujourd'hui de l'importance des projets pilotes dans les cas d'utilisation, mais si on prend l'exemple du SecureKey Service de Concierge, environ sept à huit millions d'utilisateurs y sont maintenant inscrits. Ce service a été proposé en 2012. En sept ans, donc, il a rejoint une partie importante de la population canadienne. On ne sait jamais comment un projet pilote peut prendre son envol et vraiment mettre en évidence dans la société une volonté très large de se procurer un service qui facilite la vie de tout le monde.

L'hon. Peter Kent: Encore une fois, il faut faire accepter l'idée que c'est rentable.

Mme Marina Mandal: Exactement.

Le président: Merci, monsieur Kent.

C'est maintenant au tour de Mme Vandenbeld, qui aura cinq minutes.

Mme Anita Vandenbeld (Ottawa-Ouest—Nepean, Lib.): Merci beaucoup de nous avoir fait profiter de vos compétences.

Sauf erreur, c'est vous, madame Shea, qui avez dit qu'il y aurait forcément des cyberattaques, et que l'une des meilleures façons d'affronter le problème est d'échanger des renseignements.

À qui songiez-vous, en parlant d'échange de renseignements?

Mme Della Shea: La notion d'échange de renseignements va être de plus en plus importante, et il sera très important de prendre en considération l'échange entre les divers secteurs.

Dans différents secteurs industriels, on fixe des limites à l'échange de renseignements. Chez Symcor, nous avons un cas d'utilisation limitée. Il s'agit de donner à nos clients la capacité de communiquer des renseignements de façon limitée afin de détecter la fraude, et non les cyberattaques, auxquelles nous voudrions nous intéresser aussi. Au fond, nous cherchons à avoir un processus verrouillé et contrôlé qui est très axé sur la raison d'être de chaque cas d'utilisation. Nous voulons couper l'herbe sous le pied aux acteurs malveillants ou intervenir après coup si nous n'arrivons pas à les contrer.

Il est certain que les partenariats public-privé sont un sujet de discussion au sud de la frontière. Il sera de plus en plus important d'avoir un cadre pour pouvoir communiquer ces renseignements dans cette optique.

Au-dessus de tout cela, il y a une gouvernance et une surveillance solides de la protection des renseignements personnels, parce qu'il y a souvent une tension entre la sécurité... Il nous faut le plus d'information possible afin de devancer rapidement les acteurs malveillants, mais il y a certainement un point d'équilibre qui est possible entre les deux extrêmes. Il s'agit de permettre une communication plus poussée des données, mais encadrée par une gouvernance de la protection des renseignements personnels.

● (1635)

Mme Anita Vandenbeld: Passons du secteur privé à l'appareil gouvernemental. Comment cela peut-il s'appliquer? Comme vous l'avez dit, la communication de tous les renseignements, même entre les ministères, et à plus forte raison entre le gouvernement et le secteur privé, risque de susciter beaucoup de préoccupations au sujet de la protection de la vie privée. Comment vous assurez-vous d'échanger de l'information afin de repousser les acteurs malveillants ou de vous renseigner sur ce qu'ils font, de façon à sécuriser vos systèmes, sans créer des points d'accès pour échanger de l'information?

Mme Della Shea: Il faut assurément une approche à plusieurs niveaux de l'infrastructure pour pouvoir y arriver. Il est essentiel d'intégrer à cette conception la protection des renseignements personnels. Dans le modèle estonien, chose certaine, on discute de la possibilité d'utiliser à cette fin les chaînes de blocs. Mme Cavoukian a signalé qu'il était important d'intégrer la protection de la vie privée dès le stade de la conception, et de ne pas présumer que cette protection sera assurée.

L'autre niveau concerne également le cadre législatif et la capacité de permettre l'échange d'information, mais, là encore, il faut s'adapter à chaque cas d'utilisation. Je dois souligner que la confiance est à la base de tout, et qu'il sera absolument essentiel d'avoir une raison légitime, motivée et raisonnable d'échanger ces données. La mise en oeuvre va vraiment tenir compte des utilisateurs, des processus et de la technologie habituels si nous voulons que le processus continue de fonctionner.

Mme Anita Vandenbeld: Voulez-vous répondre?

Mme Angelina Mason: Il peut y avoir des échanges qui ne portent pas sur des renseignements personnels. Au fil des ans, le secteur bancaire a établi un certain nombre de partenariats public-privé dans le cadre desquels nous avons échangé des renseignements sur les menaces. Nous pouvons donc communiquer au sujet des cybermenaces que nous observons.

Le Centre canadien pour la cybersécurité que nous avons maintenant est perçu comme la plaque tournante. Le Centre s'appuiera sur ces partenariats initiaux et leur donnera beaucoup plus d'ampleur. Il y aura donc des échanges de renseignements entre le secteur privé et le gouvernement. Il y a aussi l'avantage supplémentaire des échanges à l'échelle internationale.

Nous avons très hâte de participer aux efforts du Centre.

Mme Anita Vandenbeld: Quelle serait l'incidence des technologies émergentes? Je pense en particulier à l'intelligence artificielle. Est-ce un domaine où l'intelligence artificielle pourrait être appliquée à la détection des menaces de cette nature?

Mme Angelina Mason: Absolument. Il s'agit d'établir des liens entre les divers éléments. Plus nous pourrons exploiter l'intelligence artificielle pour analyser les faits et établir ces liens, mieux ce sera.

Mme Della Shea: Je suis tout à fait d'accord avec Mme Mason. L'intelligence artificielle et l'apprentissage automatique sont des technologies qui peuvent en fait améliorer la protection de la vie privée, puisqu'elles court-circuitent l'élément humain.

Je voudrais réaffirmer l'importance du cas d'utilisation, auquel il faut rester très fidèle. Il n'y aura pas de solution universelle. Il faut donc définir un cadre et avoir, pour chaque cas d'utilisation, un guide qui oriente le travail du début à la fin.

Le président: Votre temps de parole est écoulé. Nous venons de franchir la limite.

Il reste trois intervenants. M. Angus aura trois minutes et il sera suivi de Mme Fortier et M. Baylis. Je n'ai personne d'autre sur ma liste pour l'instant.

Monsieur Angus, à vous.

M. Charlie Angus: Merci.

Les Canadiens ont énormément de respect pour Statistique Canada, mais lorsqu'il a décidé d'échanger des données financières pour obtenir une meilleure information, il y a eu une vigoureuse réaction de rejet, ce qui donne à penser que les Canadiens sont très chatouilleux lorsqu'il s'agit de ce genre d'intégration de l'information financière avec le gouvernement.

Quelle est votre position à ce sujet? Êtes-vous sensible au fait que les gens ne veulent pas ce genre d'intégration poussée entre leurs renseignements financiers personnels et le gouvernement, même si les données sont anonymisées?

● (1640)

Mme Angelina Mason: Oui, nous sommes très sensibilisés au problème. Je souligne d'abord que, lorsque Statistique Canada a décidé d'obliger les banques à lui communiquer des données, nous n'étions pas au courant de ce qui se passait. Lorsque la chose s'est produite, nous avons évidemment eu de graves préoccupations.

Tout d'abord, je tiens à préciser qu'aucune donnée sur les opérations financières personnelles n'a été fournie à Statistique Canada. Nous étions très soucieux de la protection de la vie privée et de la sécurité des renseignements de nos clients et nous avons été évidemment très rassurés de voir le Commissariat à la protection de la vie privée mener une enquête à ce propos.

Il y a une certaine méfiance, c'est sûr, à ce niveau de données. Le secteur bancaire entretient depuis longtemps des relations avec Statistique Canada, à qui il fournit des renseignements utiles, mais il s'agissait toujours jusqu'ici de données agrégées, comme les taux de défaut de paiement hypothécaire. La nature de la demande suscitait chez nous de profondes préoccupations. Nous pensions que nos discussions en étaient à l'étape exploratoire, et nous faisions beaucoup de mises en garde. Nous avons évidemment été très étonnés que les choses se passent ainsi.

M. Charlie Angus: Merci. En fait, c'est très rassurant d'entendre votre réponse, car nous avons entendu de nombreux Canadiens exprimer une vive inquiétude.

Je voudrais terminer en revenant à mon point de départ: la fraude. Le Comité a étudié les dangers et la puissance de l'intelligence artificielle, qui va transformer tout ce qui passe en ligne. Notons les hypertrucages et la capacité de pratiquer un ciblage de plus en plus précis grâce à des renseignements personnels de plus en plus nombreux. C'est pourquoi le non-respect des renseignements personnels présente un si grand danger à notre époque.

Je m'intéresse à la formation. Il peut arriver qu'un client d'une banque fasse beaucoup d'opérations louches parce qu'il a un problème de jeu, ce qui n'est pas forcément illégal, mais un autre client, victime d'exploitation, peut vouloir faire beaucoup de retraits pour payer quelqu'un qui n'existe pas, qui dirige un gang criminel en Europe de l'Est. Quelqu'un a peut-être produit un hypertrucage dont le personnage dit avoir besoin de cet argent, mais il est en Europe.

Il y a toutes sortes de nouveaux éléments que nous n'avons pas abordés jusqu'ici. Comment formez-vous votre personnel, qui est en première ligne et devra affronter beaucoup de problèmes de cet ordre? Donne-t-on de la formation aux caissiers? Exercez-vous une surveillance aux caisses?

Mme Angelina Mason: Oui, le personnel de la banque se réunit pour examiner les signalements de comportements inhabituels. Il y a aussi des déclencheurs électroniques. Lorsqu'il y a des opérations inhabituelles dans un compte, elles sont retirées. Il y a à la fois des observations faites par des humains et une surveillance électronique.

Le président: Merci, monsieur Angus.

La dernière personne à intervenir aujourd'hui sera Mme Fortier.

[*Français*]

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

Je vous prie d'excuser mon retard, dû à un contretemps dans ma circonscription.

Mesdames, j'ai malheureusement raté vos présentations orales et je me suis servie de vos notes pour préparer mes deux questions. J'espère donc ne pas vous obliger à vous répéter dans vos réponses.

Madame Shea, mes questions s'adresseront à vous.

Si vous voulez également intervenir, mesdames Mason et Mandal, je vous invite à le faire.

Madame Shea, vous écrivez dans votre présentation que « le gouvernement étudie la meilleure approche de prestation des services » et que vous lui proposez donc « d'adopter un modèle de gérance des données ». Pourriez-vous préciser deux ou trois avantages que le gouvernement aurait à adopter une telle approche, mais aussi les risques que celle-ci soulèverait?

[*Traduction*]

Mme Della Shea: Voulez-vous parler des risques que comporterait l'adoption d'une approche uniforme?

[*Français*]

Mme Mona Fortier: Oui. Cette approche comporte-t-elle des risques?

[*Traduction*]

Mme Della Shea: Je veux m'assurer de bien comprendre. La question porte sur la mise en place de systèmes et les risques que cela présente?

Mme Mona Fortier: On dit ici que vous voulez adopter un modèle de gérance des données. Y a-t-il des risques dont nous devrions tenir compte si nous adoptions ce type de modèle?

● (1645)

Mme Della Shea: Bonne question. Je ne vois pas que l'adoption d'un modèle de saine gouvernance des données, de saine gestion des données puisse présenter des risques. En implantant ces contrôles, ces méthodes et ces processus, on place le gouvernement dans une situation gagnant-gagnant, en fait.

Le cas de Statistique Canada, comme M. Angus l'a dit, est un exemple de cas où l'objectif légitime que pouvait avoir l'échange proposé n'a pas été pris en compte. Beaucoup de questions auraient pu être mieux étudiées. On aurait pu, d'abord et avant tout, définir un objectif légitime et formuler des demandes d'information fondées et raisonnables. Ensuite, on aurait pu mettre en place un processus de gouvernance sain pour faire en sorte que, quelle que soit l'utilisation, il y ait de la cohérence et qu'on puisse agir en conséquence.

[*Français*]

Mme Mona Fortier: Je passe à ma deuxième question. En fonction de l'expérience que vous avez acquise lors de la transition de votre entreprise, Symcor, de l'imprimé vers le numérique, quels éléments devrions-nous prendre en considération alors que nous déterminons la stratégie de gestion du changement à adopter dans le cadre de la numérisation des services gouvernementaux?

[*Traduction*]

Mme Della Shea: Je vous remercie de cette question, qui est excellente, car il ne faut pas sous-estimer l'importance de la gestion du changement au moment de passer d'un service traditionnel à un service numérique. Fondamentalement, on introduit beaucoup de choses nouvelles dans un ensemble existant d'intervenants qui ne sont pas nécessairement conscients de la façon dont ces technologies fonctionnent, des raisons pour lesquelles ils devraient les utiliser et de l'incidence qu'elles auront sur leur vie.

Comprendre cela dès le départ et avoir un programme et un mandat de gestion du changement pour s'assurer de mobiliser tous les intervenants de l'entreprise, ou, dans ce cas-ci, des services gouvernementaux, et pour offrir la formation et la sensibilisation voulues, voilà qui devient très important. De plus, cette formation et cette sensibilisation doivent être constamment reprises, et à un niveau très élémentaire, pour que tout le monde comprenne.

Il importe également de reconnaître que le rythme de l'adoption ne sera pas partout le même. Il y aura des adopteurs précoces et des retardataires, et il sera essentiel d'avoir un mécanisme pour faire participer tout le monde à ce cheminement.

[*Français*]

Mme Mona Fortier: Madame Mason ou madame Mandal, souhaitez-vous ajouter quelque chose en lien avec la gestion du changement?

[*Traduction*]

Mme Marina Mandal: L'ABC est d'accord avec Mme Shea.

Notre association travaille beaucoup à la littératie financière. On peut soutenir qu'il faut une éducation semblable dans le domaine des données et du numérique pour amener les Canadiens à comprendre ce qui se passe lorsqu'ils transmettent de l'information, qu'il s'agisse de renseignements financiers personnels ou de renseignements sur la santé, etc.

Le volet de la littératie — Mme Shea en a parlé à propos de la formation et de la sensibilisation — me semble vraiment crucial. Nous revenons toujours au fait que les innovations ne seront pas adoptées si elles ne gagnent pas la confiance des Canadiens. Je confirme simplement que je suis d'accord.

[*Français*]

Mme Mona Fortier: Merci beaucoup.

[*Traduction*]

Le président: Merci, madame Fortier.

Monsieur Erskine-Smith.

M. Nathaniel Erskine-Smith: J'ai donné avis de ma proposition mardi. Puisqu'il nous reste du temps, je voudrais présenter une motion pour inviter les cadres supérieurs de YouTube à expliquer leur décision de ne pas diffuser de publicités politiques au cours des prochaines élections fédérales et leur refus de se conformer au projet de loi C-76.

Le président: Quelqu'un veut intervenir?

Monsieur Angus.

M. Charlie Angus: C'est une excellente motion. Je voudrais que YouTube vienne nous parler d'un certain nombre de questions. Pourrions-nous ajouter à la motion « pour discuter de tout autre enjeu », de façon que nous ne soyons pas strictement...

M. Nathaniel Erskine-Smith: Cela me convient.

M. Charlie Angus: Nous voudrons peut-être aborder d'autres questions.

M. Nathaniel Erskine-Smith: Bien sûr.

Le président: Avez-vous une motion amendée ou voulez-vous intégrer ce passage à votre motion initiale?

M. Nathaniel Erskine-Smith: Bien sûr. Je dirai simplement « invite des cadres supérieurs de YouTube Canada pour qu'ils expliquent leur décision de ne pas diffuser de publicités au cours de la campagne électorale à venir et leur refus de respecter les dispositions du projet de loi C-76 et pour discuter de tout autre enjeu relevant du Comité. »

● (1650)

Le président: Monsieur Kent, avez-vous quelque chose à dire?

L'hon. Peter Kent: Oui, je suis tout à fait d'accord. J'appuierais certainement cette motion, mais comme je crois l'avoir dit à la dernière réunion, nous devons également inviter le directeur général des élections et le commissaire à la protection de la vie privée à venir nous expliquer leur interprétation de ce que le projet de loi C-76 exigera des partis et des hommes et femmes politiques, à titre individuel, en matière de protection des données. Cela pourrait se greffer à motion sur YouTube.

Le président: À mon avis, il faudrait une motion distincte. Proposeriez-vous une motion distincte?

L'hon. Peter Kent: Eh bien, il y a une série de témoins qui sont tous liés dans cette affaire. Selon moi, il serait pertinent de faire un ajout à la motion. Pourrait-il s'agir d'un amendement favorable?

M. Nathaniel Erskine-Smith: Pourquoi ne pas commencer par ce que je propose, puis nous pourrons discuter entre nous de la façon dont les choses évoluent.

L'hon. Peter Kent: L'intention de continuer avec ceci... oui.

Le président: D'accord.

Monsieur Angus.

M. Charlie Angus: Oui, c'est ce qui semble le plus facile. La porte est ouverte. Nous n'avons pas besoin d'une étude complète.

L'hon. Peter Kent: Oui, je suis d'accord.

M. Charlie Angus: Cela pourrait nous amener à aborder différentes questions. Allons-y, et nous verrons de quel côté nous allons.

Le président: Est-ce acceptable, monsieur Kent? Sinon, il est possible de présenter une autre motion.

L'hon. Peter Kent: Étant donné l'esprit collégial qui a toujours régné au Comité, j'accepte.

Le président: Nous allons voter sur la motion dont nous sommes saisis.

(La motion est adoptée. [*Voir le Procès-verbal*])

M. Nathaniel Erskine-Smith: Une dernière chose.

Dans son livre blanc, l'Association des banquiers canadiens a formulé quelques recommandations précises, y compris des modifications législatives qui nous permettront de nous rapprocher de l'identification numérique. Je reconnais que le Cadre de confiance pancanadien est la prochaine étape, mais étant donné qu'il y a des recommandations précises qui n'ont pas été abordées dans votre déclaration liminaire et dont vous n'avez pas parlé en répondant aux questions — comme la recommandation proposant des modifications législatives —, il serait utile, lorsque nous formulerons des recommandations à l'intention du gouvernement, que vous fassiez un suivi par écrit si vous pensez que le Comité devrait faire certaines recommandations précises au gouvernement. C'est un exemple, et il y en a peut-être d'autres. Je vous en serais reconnaissant.

Mme Angelina Mason: Oui, bien sûr.

Le président: Est-ce tout, mesdames et messieurs?

Merci à tous. Bon week-end.

La séance est levée.