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 139 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 28 février 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 28 février 2019

● (1530)

[*Traduction*]

Le vice-président (M. Charlie Angus (Timmins—Baie James, NPD)): Bonjour. Nous allons commencer.

[*Français*]

Je voudrais d'abord faire une annonce. Il y a eu une révolution et je suis le nouveau capitaine de ce comité. Les anarchistes sont arrivés.

Un député: Temporairement.

[*Traduction*]

Le vice-président (M. Charlie Angus): Bienvenue, mes amis, au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. Il s'agit de la réunion 139, conformément à l'article 108(3)h)(vii) du Règlement, pour l'étude sur la protection des données personnelles dans les services gouvernementaux numériques.

Aujourd'hui, nous recevons deux groupes de témoins. Nous avons, du Herjavec Group, Matthew Anthony, vice-président, Cas d'incident et analyse des menaces, et Ira Goldstein, vice-président directeur, Expansion de l'entreprise. Nous avons également, de SecureKey Technologies Inc., Andre Boysen, dirigeant principal de l'information, et Rene McIver, chef de la sécurité.

Chaque groupe aura 10 minutes pour présenter son exposé. Nous sommes raisonnables, mais quand vous approcherez des 10 minutes, je commencerai à m'agiter bruyamment, non pas pour vous distraire, mais pour que vous le sachiez. Ensuite, nous aurons notre première série de questions de sept minutes, puis une série de cinq minutes.

Le Herjavec Group est-il prêt à commencer?

M. Ira Goldstein (vice-président directeur, Expansion de l'entreprise, Herjavec Group): Bonjour. Je remercie le président, les vice-présidents et les membres du Comité de nous donner l'occasion de nous exprimer aujourd'hui.

Je m'appelle Ira Goldstein. Je suis vice-président directeur à l'Expansion de l'entreprise du Herjavec Group. Je travaille depuis 10 ans dans la sécurité de l'information afin d'aider les entreprises et les gouvernements à sécuriser leurs actifs numériques les plus précieux.

Je suis accompagné de Matt Anthony, vice-président chargé des mesures correctives en matière de sécurité dans notre groupe, qui s'exprimera après moi.

Le Herjavec Group a été fondé en 2003 par Robert Herjavec, qui a immigré au Canada avec ses parents d'Europe de l'Est. M. Herjavec, entrepreneur dynamique, a fait du Herjavec Group une des plus grandes sociétés privées du monde dans le domaine de la cybersécurité. Nous travaillons avec des organisations des secteurs public et privé dans des environnements multi-technologies complexes afin de garantir la sécurité et la confidentialité de leurs données.

C'est un honneur pour nous de témoigner devant le Comité aujourd'hui au nom de M. Herjavec, du Herjavec Group et de nos concitoyens.

Notre exposé portera sur deux sujets liés à l'étude du Comité. J'expliquerai d'abord que l'identité numérique est un élément essentiel de la transformation des services gouvernementaux. Ensuite, je présenterai les étapes de la gestion et de la sécurisation de nos identités numériques.

Je recommande au gouvernement de procéder avec circonspection sur la voie de la transformation plus générale afin de s'assurer que la protection des données personnelles et la sécurité viennent en tête des priorités. Parallèlement, le gouvernement devrait mettre sur pied sans tarder un projet pilote afin d'élargir le succès existant de la présence numérique du Canada.

Les services gouvernementaux numériques doivent reposer sur une bonne gestion des identités. Si leur identité doit être numérisée et gérée par le gouvernement, les citoyens s'attendent à un système qui garantisse la sécurité et la protection des renseignements personnels. Nous partons du principe que l'émetteur, notre gouvernement fédéral, protège les attributs de notre identité. Dans tout système, physique ou numérique, la fraude est un risque qui doit être atténué par une évaluation efficace et continue.

Ces concepts ne sont pas loin de se réaliser. Quand un enfant naît ou qu'un nouvel immigrant arrive, il est possible de demander des pièces d'identité en ligne. Ensuite, des objets physiques sont délivrés comme preuve d'identité, mais le fait que nous ayons aujourd'hui un portail en ligne pour fournir des pièces d'identité signifie que nous avons les bases pour tirer parti de ces données pour une utilisation dans les services gouvernementaux en ligne.

Plusieurs services gouvernementaux sont déjà en ligne. Une des fonctions les plus essentielles du gouvernement, la perception des impôts, est numérisée dans le cadre du système TED de l'Agence du revenu du Canada. On peut penser que la perspective de gains d'efficacité a facilité l'adoption de TED, qui est un cas de transformation numérique réussie.

Toute autre mesure visant à numériser l'identité des citoyens doit prendre en considération la perception des répercussions sur la protection des renseignements personnels. Malgré les avantages escomptés, certains peuvent voir dans l'identité numérique une menace à leur vie privée. J'en veux pour exemple récent la vitesse à laquelle la perception du public s'est détériorée lorsqu'il a été question que Statistique Canada collecte des données financières personnelles. Malgré l'intervention du commissaire à la protection de la vie privée et les mesures prévues pour rendre les données anonymes, la perception est vite devenue négative à cette perspective.

Le contraste entre le succès de TED de l'Agence du revenu du Canada et la tentative de Statistique Canada de collecter des données financières devrait guider le Comité. La numérisation des services gouvernementaux sera bien accueillie par le public si elle fait l'objet d'une gestion et de messages mûrement réfléchis. Cette démarche a pour aspect positif d'améliorer l'accès de groupes historiquement et géographiquement marginalisés, ce qui fait qu'on ne peut ignorer l'occasion qui se présente.

De tout temps, la vérification d'identité a nécessité qu'un pouvoir centralisé fiable régisse la fourniture et l'utilisation des pièces d'identité. Si je veux prouver qui je suis, je dois présenter une pièce d'identité délivrée par le gouvernement. Je prédis que cette preuve officielle demeurera une caractéristique permanente de la démocratie moderne. Par conséquent, malgré les progrès de l'identité décentralisée, le gouvernement a un rôle important à jouer dans la gestion de l'identité.

En résumé, je recommande vivement que le Comité saisisse l'occasion de poursuivre la numérisation des éléments de l'identité des citoyens afin de permettre la prestation efficace et sûre des services gouvernementaux, tout en étant prudent quant à la limite à établir entre la centralisation des données et la protection des renseignements personnels à assurer.

● (1535)

M. Matthew Anthony (vice-président, mesures correctives en matière de sécurité, Herjavec Group): Merci, Ira.

Je m'appelle Matt Anthony. Je suis vice-président chargé des mesures correctives en matière de sécurité. Je travaille dans la sécurité de l'information depuis plus de 20 ans. C'est un honneur pour moi de témoigner devant le Comité aujourd'hui. Mes observations porteront sur deux principaux domaines.

Je parlerai d'abord de la question du cybergouvernement, en particulier le rythme du changement et son volume. De grands succès ont été enregistrés. Ira a déjà mentionné la production des déclarations de revenu. On peut tout faire, de la production des déclarations de revenu à l'enregistrement des animaux, à tous les paliers de gouvernement. Nous voyons, selon moi, de réels avantages à certaines de ces démarches, mais je vois aussi que la peur de se priver de quelque chose et l'amélioration de la réputation sont les moteurs de bon nombre des initiatives qui influencent l'adoption des services gouvernementaux électroniques et l'adaptation à ces services.

Mark Zuckerberg, le fondateur de Facebook, est célèbre pour avoir dit qu'il faut aller vite, quitte à tout casser. Dans le monde entier, les concepteurs en ont fait un mantra dans tous les domaines des affaires et dans le secteur privé, mais je ne pense pas que le gouvernement du Canada devrait ou pourrait avoir le même type de capacité d'aller vite, quitte à tout casser. Les équipes d'intervention du Herjavec Group en cas de cyberincident voient les conséquences directes quand on est allé vite, quitte à tout casser. Nous revenons recoller les morceaux. Les atteintes à la sécurité sont importantes, coûteuses et très préjudiciables.

En plus, il y a une pénurie générale de compétences dans les capacités principales nécessaires pour gérer, développer, essayer, déployer et entretenir en toute sécurité des systèmes logiciels complexes. Les chiffres actuels publiés montrent qu'on offrira environ 3,5 millions d'emplois dans la cybersécurité d'ici 2021, dans le monde, évidemment. La transformation numérique mondiale est en tension directe avec cela. Il y a plus de projets, plus de services et plus de données créées, entreposées, gérées et exploitées. Le Canada et les administrations canadiennes ressentiront très directement cette tension.

Le Comité a beaucoup entendu parler de trois études de cas. Ira l'a déjà mentionné et j'ai entendu parlé de deux d'entre elles dans les couloirs. Il s'agit de Sidewalk Toronto, de l'Estonie et de l'Australie.

Je parlerai brièvement de l'exemple de l'Estonie parce qu'on le considère comme un record en matière de transformation numérique. Cependant, l'Estonie a engrangé au passage des avantages importants que ne connaît pas le Canada. Le pays est peu peuplé, a une très petite superficie, est assez neuf sur le plan technologique à l'ère post-soviétique et a une population assez homogène habituée à un contrôle central.

Quand je parle de ces choses, je pense qu'on peut réfléchir au fait que le Canada n'a pas beaucoup de ces avantages quand il essaie d'offrir ces genres de services. Le modèle serait très différent au Canada.

Cette transformation semble réussie, mais nous n'en savons pas beaucoup sur les problèmes de sécurité et de protection des renseignements personnels. On ne connaîtra probablement pas avant des années, voire plus, les aspects politiques et culturels relatifs aux attentes, et on devra probablement aussi attendre pour en apprendre plus au sujet des aspects liés à la sécurité et à la protection des renseignements personnels. Je mets en garde contre la tentation de prendre l'Estonie comme point de référence pour nos transformations au Canada.

On ne peut pas rester sans rien faire, c'est évident, et nous devons avancer, mais j'espère que nous procéderons assez lentement pour nous assurer que les changements que nous opérons sont entièrement régis et garantis comme il convient. Il faut procéder doucement en suivant des principes rigoureux. Il faut attendre que la technologie nécessaire, comme l'IA et les commandes d'automatisation, soit prête à mieux nous soutenir. Il ne faut pas laisser la peur d'être à la traîne dans les comparaisons internationales nous pousser à nous précipiter sans avoir les capacités voulues.

Ensuite, je parlerai brièvement de l'échange d'information. Je tiens à saluer la feuille de route de la Stratégie de données pour la fonction publique fédérale, car il y est question de cinq ou six choses importantes. Je me contenterai de dire qu'elles sont précises et correctes. J'aimerais cependant entrer dans plus de détails.

Les concepts sont simples: définir une stratégie; préciser davantage qui est responsable des données; définir des normes et des lignes directrices en matière de gouvernance; améliorer le recrutement afin de réunir les compétences nécessaires; et créer des systèmes technologiques à l'appui de la stratégie. Tout cela est facile à dire, mais beaucoup plus difficile à faire, individuellement et solidairement.

En 1984, Stewart Brand écrivait de façon prémonitoire que l'information veut être libre. Parallèlement, il expliquait comment le coût de la technologie ne cessait de baisser, mais à présent, cela est devenu synonyme de difficulté à contrôler l'accès. Une fois que le contrôle de l'information échappe à sa source, ladite information tend à être largement diffusée. Il faut donc que l'utilisation secondaire et tertiaire des données gouvernementales soit contrôlée d'aussi près que l'utilisation primaire.

Le gouvernement est confronté à une tâche monumentale pour ce qui est de comprendre et de gérer les données et les systèmes anciens. Rapprocher les consentements à l'utilisation contradictoires ou non consignés, le cloisonnement de l'information, les règles d'utilisation, les structures de données, les plateformes d'identité et les processus administratifs, la tâche sera immense dans chacun de ces aspects.

Il peut être avantageux, selon moi, d'adopter une approche nouvelle, c'est-à-dire d'établir clairement les règles pour la collecte de nouvelles données et autoriser dans le futur l'intégration des données anciennes, lorsqu'il sera possible d'associer des capacités telles que l'IA et la collecte et le marquage d'autres données avec des coûts inférieurs pour la transformation, grâce à l'automatisation. Ne vous précipitez pas sur les modèles de type lacs de données, car il se produira une dé-anonymisation et une mise en corrélation d'information imprévues — je l'ai vu arriver — parfois contraires à l'intérêt public, à la loi ou à l'intention.

● (1540)

Beaucoup déclarent que l'extraction, l'agrégation et le partage actifs de données ouvriront des possibilités et permettront des gains d'efficacité. Je demande instamment au Comité d'en montrer la preuve. Il est facile de se laisser tenter par cette approche.

On ne peut pas rester sans rien faire, mais je conseille, en fait, j'encourage le Comité et l'industrie à ralentir, à se montrer plus prudents et à ne pas laisser l'ambition l'emporter sur les capacités. Allez assez lentement pour bien comprendre, mesurer et gérer les risques liés à l'information. Rappelez-vous que les criminels aiment les données et que les atteintes à la sécurité sont compliquées et très coûteuses.

Je vous remercie.

Le vice-président (M. Charlie Angus): Je vous remercie.

Nous allons passer à SecureKey Technologies. Vous avez la parole.

Mme Rene McIver (chef de la sécurité, SecureKey Technologies Inc.): Bonjour. Je m'appelle Rene McIver, je suis chef de la sécurité et agente à la protection de la vie privée chez SecureKey.

Je tiens d'abord à remercier le Comité de nous donner l'occasion de participer à son étude sur la protection des renseignements personnels dans les services gouvernementaux numérisés. Je suis spécialisée dans les crypto-mathématiques, les normes biométriques et l'identité. J'ai travaillé au Centre de la sécurité des télécommunications et je travaille chez SecurKey depuis 10 ans.

Je suis accompagnée aujourd'hui par mon collègue Andre Boysen, notre dirigeant principal de l'information et cofondateur de SecureKey. M. Boysen travaille dans le secteur de la technologie financière depuis 30 ans et est un chef de file mondialement reconnu dans le domaine de l'identité numérique et de la protection des renseignements personnels. Il siège par ailleurs au conseil d'administration du Digital ID & Authentication Council of Canada.

SecureKey est une fière entreprise canadienne. Depuis 2012, elle est le fournisseur officiel de service de partenaire de connexion du gouvernement du Canada, aussi appelé Service de concierge. Nous sommes parmi les leaders mondiaux dans la fourniture de solutions technologiques qui permettent aux citoyens d'accéder efficacement à des services numériques de grande valeur, tout en assurant la sécurité de l'information et en protégeant leurs renseignements personnels. Pour cela, nous créons des réseaux hautement sécurisés qui conjuguent les points forts des secteurs public et privé.

Comme nous le savons, l'ère numérique a permis de créer quantité de nouveaux services, de modèles d'entreprise et de possibilités de participer aux activités internationales. Il n'y a pas longtemps encore, il aurait été inimaginable de commander un covoiturage sur un appareil qui tient dans la poche ou d'accéder en toute confidence à des services gouvernementaux, de chez soi. Aujourd'hui, nous tenons ces choses pour acquises et souvent, nous sommes irrités quand nous tombons sur quelque chose qui ne peut pas être fait en ligne.

Il ne s'agit pas seulement des attentes des citoyens. Les entreprises, les gouvernements et d'autres organisations ont de très bonnes raisons de mettre en ligne des services et des transactions, comme améliorer l'expérience du client, réaliser des économies et accroître la sécurité des activités. La capacité d'une organisation de faire cela repose sur une seule question: est-ce que je peux faire confiance à la personne ou à l'identité numérique à l'autre bout de la transaction?

Le défi de l'identité numérique est tout aussi problématique des deux côtés.

Pour reconnaître les clients et leur fournir un accès fiable à des services en ligne, les organisations déploient généralement un ensemble de mesures analogiques et numériques afin de confirmer l'identité et d'atténuer les risques. Comme nous l'avons vu, cependant, ces solutions tendent à être complexes et inadéquates. Résultat, elles inspirent moins confiance.

En revanche, on demande aux citoyens de se soumettre à quantité de méthodes d'identification pour satisfaire les organisations dont ils sollicitent les services, sans savoir où va l'information et alors qu'on ne cesse de révéler des atteintes à la sécurité des données et que les imposteurs en ligne sont toujours plus nombreux.

Ces préoccupations sont tout à fait fondées. Les fraudeurs recueillent des données pour en savoir autant et parfois plus que les citoyens dont ils usurpent l'identité. Les cartes physiques standard sont faciles à contrefaire et il est souvent impossible de vérifier leur validité auprès des émetteurs. Même les méthodes biométriques, qu'on vante souvent comme étant la solution à la fraude numérique, sont la cible des pirates, ce qui augmente le risque que des données biométriques soient compromises.

Ces facteurs augmentent la complexité, font douter du système et nuisent à la protection des renseignements personnels, ce qui est exactement l'inverse de ce qui doit se passer. Notre système cloisonné est trop difficile à utiliser pour les consommateurs et trop cher à maintenir.

Le défi pour nous n'est pas seulement de trouver la meilleure technologie, les bonnes compétences ou suffisamment de fonds pour corriger les problèmes; en fait, quiconque a un intérêt dans le système doit chercher à résoudre le problème de l'identité numérique qui sous-tend tous les services numériques. Nous devons redonner au citoyen le contrôle des données et des renseignements concernant l'identité.

Pour relever ce défi, nous devons trouver des moyens d'associer les principaux facteurs de l'identité. Ces facteurs sont les choses uniques que nous connaissons, comme des secrets partagés; les choses uniques que nous avons, comme les cartes à puces vérifiables et les appareils mobiles; et les choses uniques que nous sommes, comme nos empreintes digitales ou nos images faciales. En combinant ces facteurs, nous pouvons résoudre le problème de l'identité et faire en sorte que les organisations sachent que leurs clients sont bien qui ils disent être.

L'expérience à ce jour montre que les méthodes à facteur unique ne suffisent pas. Il faut donc des réseaux sécurisés, autrement dit des écosystèmes de participants de confiance. Tous les participants doivent participer à la solution, y compris, et peut-être surtout, les citoyens, dont le contrôle de leurs propres données et la protection de leurs renseignements personnels en garantiront la sécurité.

● (1545)

Ce n'est qu'en associant les meilleurs aspects de tous les systèmes que nous réglerons le problème de l'identité et que nous rebâtirons la confiance dont ont tout autant besoin les organisations et les citoyens. Par exemple, les gouvernements sont les premiers émetteurs de documents d'identité, y compris les registres des naissances, les documents d'immigration, les permis et les licences. Ils peuvent également relier leurs dossiers à une personne vivante en délivrant un permis de conduire ou un passeport. Mais ils ne sont pas aussi aptes que le secteur commercial à savoir si cette personne est bien à l'autre bout de la transaction numérique. Les banques, toutefois, réussissent à effectuer des milliards d'authentifications par an.

En comparaison d'autres organisations, les citoyens ne sont que rarement en contact avec les administrations durant leur vie. Il leur arrive de renouveler un permis ou un passeport tous les cinq ans ou de payer des impôts en ligne une fois par an, mais ils se connectent plusieurs fois par semaine à leurs comptes bancaires. Cette fréquence renforce le degré de confiance et confère à cette interaction plus d'instantanéité.

Pensez aux appareils mobiles, qui sont à la fois identifiables dans un réseau cellulaire et rattachés aux comptes de l'abonné par la carte SIM de l'utilisateur. Tous les éléments ont quelque chose d'utile à offrir au sein d'un réseau performant.

Imaginez un scénario où les citoyens puissent choisir de partager l'information en toute sécurité à l'intérieur d'un réseau constitué d'organisations en qui ils ont déjà confiance. Cela permet d'utiliser une approche multiniveaux de la justification de l'identité. Les citoyens accéderaient au réseau en utilisant sur un appareil mobile leurs identifiants de connexion bancaire fiables que l'opérateur de télécommunications pourra valider, le tout pour partager des données fiables de multiples sources, y compris des renseignements figurant sur des documents numériques émis par le gouvernement. En utilisant cette approche multiniveaux, nous obtenons un degré de confiance nettement supérieur dans l'identité de la personne qui effectue la transaction.

La difficulté, c'est d'y parvenir sans devenir un réseau de surveillance ou sans constituer un nouveau trésor de données. Nous devons établir les bases de la protection des renseignements personnels et de la confiance, tout en réduisant au minimum le partage de données entre les parties.

La protection des renseignements personnels en triple aveugle résout ce problème. L'organisation qui reçoit les renseignements n'a pas besoin de connaître l'émetteur même de l'information, il lui suffit de savoir qu'elle vient d'une source fiable. L'émetteur n'a pas besoin de savoir qui est l'organisation qui reçoit les renseignements. Et les exploitants de réseau ne sont pas exposés aux renseignements personnels non protégés. Voilà comment fonctionne l'approche en triple aveugle.

Autrement dit, aucun des participants à la transaction ne voit, en fait, la totalité de la transaction de l'utilisateur. Cette formule éprouvée est saluée par les spécialistes de la protection des renseignements personnels dans le monde entier, y compris par le commissaire à l'information et à la protection de la vie privée de l'Ontario.

On ne parle pas d'un avenir lointain. Toutes les pièces sont déjà en place pour être capable d'utiliser un système dont l'information est fiable, qui permet à ses destinataires d'avoir confiance dans la transaction et aux citoyens d'avoir totalement confiance dans le système, car ils contrôlent leurs propres données d'une manière qui renforce la protection de leurs renseignements personnels. Ce type d'agencement est à la pointe de ce qui se fait et est actuellement utilisé.

Avec l'information et les ressources dont nous disposons, le Canada a la possibilité de régler le problème de l'identité numérique et de devenir le modèle dont le reste du monde peut s'inspirer. Nous avons des administrations qui coopèrent, des télécommunications avancées sur le plan technologique et un leadership mondial dans le développement de nouvelles approches, comme la confidentialité et la sécurité des renseignements personnels assurés dès la conception, approche mise au point par Ann Cavoukian, et aussi le cadre de fiabilité pancanadien que promeut le Digital Identification and Authentication Council of Canada. Nous avons l'occasion de créer des services capables de présenter les demandes de validation d'identité de multiples parties en une seule transaction, tout en garantissant au citoyen le plein contrôle et l'entière protection des renseignements personnels.

Les facteurs clés du succès de toute solution seront l'acceptation et la confiance des citoyens et le potentiel d'atteindre rapidement un grand nombre d'utilisateurs.

La responsabilité de protéger les renseignements personnels et de donner aux citoyens un sentiment de sécurité est essentielle au succès de toute solution. Il est vital que l'approche du Canada relie ensemble les parties fiables de l'économie numérique, comme la finance, les télécommunications, le gouvernement et le commerce. C'est le seul moyen de donner aux citoyens la confiance qu'ils exigent pour utiliser les fournisseurs auxquels ils se fient déjà et pour avoir accès à l'information qu'ils souhaitent partager de façon sécuritaire.

Les cyberrisques sont grands pour l'identité numérique. Le succès de toute solution à laquelle ne participent pas le secteur privé et le secteur public sera limité. L'approche compartimentée aujourd'hui malmenée sera perpétuée. Elle n'offrira pas la sécurité et n'aura pas la confiance du public nécessaires à l'économie numérique de demain.

Je vous remercie.

● (1550)

[*Français*]

Le vice-président (M. Charlie Angus): Nous allons commencer la période des questions.

Je vous cède la parole, madame Fortier.

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

Je vous remercie, chers témoins, d'être présents. Je vois que vous avez un niveau d'expertise supérieur au mien. Je suis très contente de constater que vous possédez une expertise qui nous permettra d'aller plus loin dans cette étude et d'accomplir ce que nous voulons faire.

Monsieur Anthony, votre expertise est très importante pour le Comité. Vous avez dit qu'il était important d'aller lentement, ce qui est intéressant. Toutefois, il faut aussi aller sûrement. C'est ce que je comprends.

Dans la société, tout va très vite présentement. Il y a une certaine pression qui nous pousse à vouloir aller plus vite pour pouvoir répondre aux besoins des Canadiens et des Canadiennes sur le plan des services numériques.

Comment pouvons-nous établir un équilibre pour bien faire les choses? Si nous procédons lentement, quels services gouvernementaux devrions-nous mettre en avant en premier, selon vous?

● (1555)

[*Traduction*]

M. Matthew Anthony: Je crains qu'il s'agisse d'une question très précise à laquelle je n'ai pas de réponse très précise. C'est ainsi qu'on concilie un défi très complexe à plusieurs variantes avec une stratégie claire et simple.

Quand Rene Heller, de l'Institut Max Plank, décrit le piège de l'innovation, il explique que peu importe le moment où on veut lancer un vaisseau spatial pour un voyage interstellaire, mieux vaut toujours attendre parce qu'on se dépassera toujours à cause de l'évolution de la technologie.

C'est ce qui arrive aussi quand on se demande si on doit acheter un ordinateur personnel ce mois-ci ou le mois prochain. C'est le même genre de piège de l'innovation.

Nous sommes confrontés à ce dilemme en politique publique aussi, lorsque nous prenons au cas par cas des décisions réfléchies par rapport aux données qui ne nous poseraient pas de problème ou à la possibilité de suffisamment contrôler les aspects nécessaires de la sécurité de l'information et de la protection des renseignements personnels avant de décider d'aller de l'avant. Il faut faire la recherche continuellement, ce qui est la partie où l'on procède lentement, pour déterminer si on est prêt à passer à la production, qui est la partie où l'on va vite.

Il faut aller lentement jusqu'au moment où on est prêt, puis passer à la vitesse supérieure.

[*Français*]

Mme Mona Fortier: Je comprends. Merci.

L'autre question que j'aimerais poser aux trois autres témoins concerne la cybersécurité.

On sait qu'une évolution va se produire. Jusqu'où la notion de cybersécurité peut-elle se rendre, selon vous? Existe-t-il des approches innovantes plus efficaces et plus fiables dont vous aimeriez nous faire part et que nous devrions prendre en considération?

Madame Mclver ou monsieur Boysen, voulez-vous vous exprimer en premier?

M. Andre Boysen (dirigeant principal de l'information, SecureKey Technologies Inc.): Oui. Merci de votre question, madame Fortier.

[*Traduction*]

La cybersécurité et la protection des renseignements personnels sont un sujet très complexe et, dans le modèle d'aujourd'hui, le fait que tout le monde au Canada doit comprendre la façon dont le système de sécurité fonctionne pour que celui-ci soit efficace est un défaut de conception fondamentale à mon avis.

J'aimerais revenir sur les remarques de Matt au sujet de l'Estonie. Ce pays a fait quelque chose d'extraordinaire pour lui-même, mais j'ai deux points clés à communiquer en ce qui concerne l'identification numérique. Premièrement, tous les gouvernements du monde veulent la souveraineté de leurs données d'identification numérique. Ils ne veulent pas être tributaires d'une société étrangère qui échappe à leur compétence. C'est là un défi.

Cependant, l'identité est une chose qui est très culturelle, ce qui constitue un défi encore plus grand. Ce qui fonctionne dans un pays ne fonctionnera pas nécessairement dans un autre. Ceci est particulièrement prononcé dans l'exemple de l'Estonie. En ce qui concerne les cartes d'identité nationale, je dirais qu'il n'y a que deux types de pays dans le monde: les pays qui ont des cartes d'identité nationale, et les pays qui détestent les cartes d'identité nationale. Je dirais que le Canada, les États-Unis, le Royaume-Uni, l'Australie, la Nouvelle-Zélande et de nombreux pays d'Europe sont contre l'idée d'une carte d'identité nationale.

Plusieurs raisons sont à l'origine de cet état de fait. C'est, en partie, à cause de la Deuxième Guerre mondiale. On a bien vu les préjudices causés par ces grandes bases de données de gouvernements. Le gouvernement n'avait aucune intention de causer du tort en créant ces systèmes, mais quand d'autres autorités sont venues par la suite — les Allemands —, elles ont créé toutes sortes de préjudices imprévus. On a bien vu le danger que représente le regroupement de toutes les données en un seul endroit. Je dirais que ceci, comparativement, est un meilleur mécanisme, mais je ne suis pas ici pour critiquer ce que l'Estonie a fait. Son modèle est très bon, mais son contexte culturel est différent, et je crois que Matt a fort bien souligné ce point.

Si nous voulons bien faire les choses, pourquoi ne regarderions-nous pas le système d'identification et d'authentification le plus grand et le plus réussi au monde, le système des cartes de crédit, plutôt que de contempler ce qu'a fait un pays d'un million d'habitants? Six milliards de cartes de paiement circulent dans le monde et nous ne voyons pas des manchettes toutes les semaines annonçant qu'une carte de crédit a été compromise en un endroit, ou que Starbucks a des problèmes dans un autre, ou encore que des utilisateurs ont perdu leurs cartes de crédit. Pourquoi ne voyons-nous pas cela?

En effet, le système mondial de paiement est géré d'une façon très différente du système d'identification en ligne que nous avons aujourd'hui. En tant que consommateur, je n'ai pas besoin de comprendre comment le mécanisme des paiements fonctionne. Tout ce que j'ai besoin de savoir, c'est comment passer ma carte sur le lecteur et, si j'arrive à le faire, tout est bon. Dans le domaine des cartes, nous avons accompli deux choses très intelligentes. Tout d'abord, c'est super simple pour l'utilisateur: quand il fait ceci, il sait qu'il s'est engagé, et il est donc difficile pour un escroc de profiter de lui. De plus, il n'a pas besoin de comprendre le fonctionnement. Il sait que la serveuse ne peut transformer son 10 $ à 1 000 $ après son départ. C'est la première chose qui fait que le système mondial de paiement est sûr.

La deuxième chose qui le rend sûr, c'est la présence d'un réseau de confiance en intermédiaire. L'escroc ne peut surgir au milieu et déclarer: « Je suis un escroc, j'accepte Visa. » Il faut présenter une demande pour rentrer dans le réseau et bien se comporter pour y rester.

Ce n'est pas la même chose qu'Internet. Sur Internet, c'est très différent. C'est pour des raisons de sécurité qu'aucune des banques du Canada n'envoie des messages textes à ses clients. Ces banques ne croient pas que ce genre de messages est suffisamment sûr. Malheureusement, tous les autres services le font. Facebook le fait, Apple le fait, Netflix le fait et Google le fait. Quand mon père reçoit dans son téléphone un message disant: « Activité suspecte dans votre compte. Veuillez cliquer sur l'URL www.bmo.com.escrocURL.com », mon père ne sait pas comment fonctionnent les URL, et il clique dessus en pensant que cela ira chez BMO. Malgré le fait que BMO a de très bons contrôles — soit dit en passant, il ne s'agit pas de BMO qui a d'excellents mécanismes de sécurité en vigueur —, la Banque se retrouve avec une atteinte à la sécurité sur les bras parce que mon père ne savait pas de quoi il s'agissait.

Par conséquent, cacher la complexité à l'utilisateur et disposer d'un exploitant de confiance du réseau sont des choses extrêmement importantes.

J'aimerais maintenant revenir sur une chose que Rene a mentionnée il y a quelques instants. La troisième chose qui assure la sécurité du système mondial de paiement est le comportement des utilisateurs. Quand je perds ma carte de crédit, j'appelle la banque dans les minutes qui suivent. Je n'appelle pas parce que j'avais promis de le faire; je ne me soucie pas d'eux, je ne me soucie que de moi. Je suis terrifié à l'idée que l'escroc qui a trouvé ma carte va dépenser mon argent et que j'en serai responsable. Ce comportement d'utilisateur, cet intérêt personnel, me conduit à faire ce qu'il faut et à l'annuler. C'est ce qui garantit la sécurité du système mondial de paiement, un aspect qui diffère entièrement de la façon dont nous gérons l'identification numérique aujourd'hui.

Par conséquent, si nous voulons nous inspirer d'un modèle, au lieu de regarder du côté de l'Estonie — bien qu'à mon avis, ce qu'elle a fait est très bon pour elle —, nous devrions nous inspirer et apprendre de ce que nous avons fait au Canada. Nous devrions examiner notre propre expérience ici. Tous les autres gouvernements du monde nous regardent et demandent comment nous avons réussi à établir un tel service d'ouverture de session du partenaire de connexion avec toutes les banques du Canada. C'est une chose qu'ils veulent tous. Tout le monde regarde ici et nous, nous regardons là-bas.

● (1600)

Le vice-président (M. Charlie Angus): Merci.

M. Andre Boysen: Nous avons ici des antécédents extraordinaires. Nous devons prendre appui sur eux plutôt que tenter de réinventer la roue.

Mme Mona Fortier: Merci.

Le vice-président (M. Charlie Angus): Monsieur Kent, je vais devoir retrancher pour elle une minute de votre temps. Êtes-vous d'accord?

L'hon. Peter Kent (Thornhill, PCC): L'esprit de collégialité régnant à ce comité, je partagerai le temps que vous jugez nécessaire.

Le vice-président (M. Charlie Angus): Poursuivez, poursuivez.

L'hon. Peter Kent: Je vous remercie tous de votre présence.

À ce sujet justement, l'Association des banquiers canadiens étudie un programme d'identification numérique, mais son PDG, dans un discours en janvier, a mentionné que les banques pourraient très bien avoir un rôle central dans tout élargissement du réseau national de services gouvernementaux numériques. Combien de niveaux de technologie exclusive cela exigerait-il éventuellement, et quel en serait le prix? Ou encore, diriez-vous que, après la DP, après les projets pilotes, un seul vendeur de technologie numérique sera choisi et mènera la barque à lui seul?

M. Andre Boysen: Non. En fait, je dirais que ce serait une très mauvaise chose.

Pour revenir à mon exemple du système mondial de paiement, il y a dans le monde 5 à 10 marques mondiales — Visa, Amex, MasterCard, Discover, et d'autres. Ces marques doivent leur existence au fait qu'elles servent toutes leur clientèle d'une façon légèrement différente. Certaines sont axées sur les marchands, d'autres sur les consommateurs. D'autres encore essayent de tout faire. Elles existent toutes parce qu'elles offrent leurs services de la bonne façon.

L'avantage dans ce modèle, c'est que nous pouvons tous choisir notre fournisseur de services financiers préféré, et nous ne sommes pas bloqués dans ce choix. Si l'on commence avec une banque puis découvre qu'on ne l'aime pas du tout, on peut changer de banque et poursuivre comme à l'accoutumée.

À mon avis, il serait dangereux d'avoir un fournisseur unique pour tout cela serait. Il nous faut un mécanisme ouvert pour que nous puissions avoir de multiples fournisseurs. C'est très important. Et ce mécanisme doit reposer sur des normes, et non pas sur de multiples technologies brevetées.

L'hon. Peter Kent: Cela irait contre la technologie estonienne de cartes courantes monopuces.

M. Andre Boysen: À la différence près que l'Estonie essaie de convaincre d'autres pays de faire ce qu'elle a fait, pour qu'elle ne soit pas la seule à le faire, ce qui est intelligent. Sinon, si le reste du monde s'oriente différemment, elle devra changer. Voilà pourquoi elle sillonne les routes prêchant pour sa paroisse — et le faisant très bien, à mon avis.

La même occasion s'offre à nous. Dans notre cas, si nous faisons ce que l'Estonie a fait, par exemple, et si les États-Unis décident de se diriger différemment, nous serons obligés de changer. Le Canada peut saisir l'occasion de mettre de l'ordre dans ses affaires, relancer son économie, puis faire de ceci une norme exportable et créer une norme de référence mondiale, parce que tout le monde nous regardera avec admiration, disant: « C'est super, on veut la même chose. »

C'est là l'occasion qui s'offre à nous.

L'hon. Peter Kent: Monsieur Goldstein, c'est vous, je crois bien, qui avez proposé de commencer avec un projet pilote de petite envergure. Quelle envergure entrevoyez-vous? Un seul ministère?

M. Ira Goldstein: Je crois qu'il faudrait examiner les services qui sont déjà en ligne et la capacité déjà établie au gouvernement fédéral. Le Centre canadien pour la cybersécurité a été un grand pas vers la concrétisation de cette capacité. Il y a une immense capacité, même si les Canadiens commencent tout juste à la découvrir publiquement en raison de cette annonce.

Nous devrions envisager les services gouvernementaux qui sont déjà quelque peu numérisés et voir comment nous pourrions prendre appui sur eux pour obtenir de meilleurs résultats pour les Canadiens.

J'approuve une grande partie de ce que tout le monde a dit, mais, à mon avis, interagir avec des services hors du gouvernement pourrait être la troisième ou la quatrième étape. La première étape consiste à faciliter la numérisation des services gouvernementaux qui ne sont pas présentement numérisés.

L'assurance-dépôts est une autre raison pour laquelle les gens ont tant confiance dans le système bancaire. C'est une garantie qui leur dit que si une institution financière perd de l'argent, ce n'est probablement pas le leur dans la mesure où ils ont suivi les règles du jeu.

Je répète qu'à mon avis, le gouvernement a un rôle de maître d'oeuvre important dans cette identification. Voyons ce qui est déjà numérisé au gouvernement. L'ARC est un exemple que l'on peut augmenter. Passons en revue les services fédéraux et voyons comment nous pourrions les réunir et prendre appui sur la numérisation existante.

● (1605)

L'hon. Peter Kent: Le site Web de l'Estonie nous informe que 98 % de la population a reçu une carte d'identité numérique. Compte tenu de la nature humaine du Canada — la réticence, le scepticisme, le cynisme, la peur ou le refus à l'endroit de l'identification numérique —, pensez-vous qu'il faudrait que ce soit facultatif dans tout projet pilote adopté?

M. Ira Goldstein: Quand je dis « pilote », il s'agit plus de la nature pilote de la capacité, mais celle-ci devrait être offerte à tous les Canadiens, et non pas forcément à un groupe pilote ou une province ou un groupe en particulier. Cette capacité pilote devrait porter sur un usage précis. Dans le cas de l'ARC, par exemple, on pourrait tout simplement continuer à l'augmenter.

Le citoyen ne s'inquiète pas de l'information sur lui dont dispose déjà le gouvernement. Reprenons l'exemple de Statistique Canada. Si le public s'est soulevé, c'est que les gens ont dit: « Humm, le gouvernement ne dispose pas de ce renseignement aujourd'hui. Maintenant, il le veut. C'est scandaleux. » Si nous avions déclaré...

L'hon. Peter Kent: C'était aussi l'absence de consentement.

M. Ira Goldstein: Mais si les renseignements sont anonymisés, où est ce consentement?

Si nous avions déclaré que nous adoptons les données ouvertes et recherchons certaines données regroupées et anonymisées pour faire en sorte que les services offerts soient moins coûteux, meilleurs et plus ciblés, beaucoup de gens auraient été réellement emballés. Les Canadiens sont de mentalité progressiste pour l'adoption du numérique. Il s'agit plus de la façon dont vous faites les choses plutôt que de ce que vous faites.

Quant à procéder avec circonspection, comme Matt l'a dit, il vous faut avancer lentement, planifier vos communications soigneusement, mais nous sommes tous fermement d'avis que les Canadiens sont prêts pour cela. Il s'agit simplement de la façon de le faire.

L'hon. Peter Kent: Bon.

J'ai une question du style la poule ou l'oeuf. L'Union européenne a adopté le Règlement général sur la protection des données, le RGPD. Il a été dit que le Canada traîne loin derrière en ce qui concerne la protection des renseignements personnels, ce que l'Europe vient d'instituer, peut-être excessivement, ou exagérant la protection de certains aspects. Avant que l'on ne mette en oeuvre le gouvernement numérique au Canada, devrions-nous élaborer un règlement semblable pour instituer des mesures de protection et de garantie comme celles du RGPD?

M. Ira Goldstein: C'est une vaste question.

Je ne crois pas que l'on puisse dire simplement que les lois canadiennes sur la protection des renseignements personnels sont insuffisantes. Nous avons quelques cadres stratégiques en la matière valables. Il s'agit de déterminer les définitions. Qu'est-ce que le « risque réel de préjudice grave »? Que cela signifie-t-il pour les sociétés comme celles que nous aidons, qui tentent de déterminer ce qu'elles doivent dire au gouvernement quand il y a eu atteinte à la sécurité ou à la vie privée?

Il faut faire en sorte qu'il soit plus pratique pour les sociétés et les particuliers de respecter ces cadres stratégiques. Je ne dis pas que nous devrions aller jusqu'à un RGPD. Nous avons certainement tous une opinion variée du RGPD. Matt tremble, maintenant.

Si les gens respectent le RGPD, c'est qu'il comporte des pénalités financières, et c'est pourquoi il y a un grand nombre de...

L'hon. Peter Kent: Tout à fait.

M. Ira Goldstein: ... consultants qui font beaucoup d'argent dans ce domaine et pour toutes ces questions.

Nous ne devrions pas aller jusqu'au bout dans ce sens, mais il faut faire en sorte qu'il soit plus facile pour les entreprises canadiennes de fonctionner avec ce type de règlement au Canada. Nous devons conserver ce solide cadre stratégique de protection des renseignements personnels, mais faire en sorte qu'il soit plus facile pour les entreprises d'en tenir compte.

M. Matthew Anthony: Puis-je parler un instant de la remarque d'Ira, puis répondre à votre question à savoir si nous devrions aller jusqu'au stade d'une sorte de RGPD?

La réponse est oui. La tendance mondiale à inciter les gouvernements à protéger les citoyens, contrebalancée par le fait que les citoyens sont, peut-être, de moins en moins intéressés à la protection des renseignements personnels sur le plan individuel augmente la motivation pour les gouvernements de protéger les citoyens, collectivement.

Cependant, ce qu'Ira a dit est vraiment important, et j'ai essayé d'en toucher un mot tangentiellement aussi, c'est-à-dire expliquer clairement comment manipuler et gérer les données de sorte que les personnes comprennent ce qui est attendu d'elles et comment elles doivent le faire, avant de commencer à propulser les choses dans l'univers en ligne. C'est une considération réellement très utile.

Je ne saurais vous dire si nous devrions ou non changer nos règlements, politiques et pratiques, mais il faudrait à tout le moins rendre ceux-ci transparents et plus faciles, de sorte que...

Le vice-président (M. Charlie Angus): Merci beaucoup.

C'est mon tour maintenant pendant sept minutes. Par souci d'équité, je vais placer le marteau à côté du greffier et, si je dépasse mon temps, il s'en servira pour me cogner dessus.

Je trouve cela fascinant, et M. Anthony semblait procéder avec circonspection. Je trouve cela très surprenant.

Il fut un temps où je croyais fermement à la valeur du numérique et que, dans un monde où règne le numérique, les choses iraient mieux, que nous avancerions plus rapidement. Plus je passe du temps dans ce travail, plus je deviens méfiant. Je crois que « procéder avec circonspection » est un exemple très intéressant.

J'aimerais parler un peu de l'opinion qu'ont, d'après moi, les Canadiens de la protection des renseignements personnels et de l'innovation numérique. Je bavardais avec des gens du milieu des technologies aux États-Unis, et ils me disaient être émerveillés de voir à quel point nous prenions ces choses au sérieux.

Nous avons eu une importante bataille sur les droits d'auteur numériques dans laquelle il était question de citoyens et de campagnes épistolaires. La question du ralentissement de la circulation de l'information sur Internet a été toute une affaire. C'est le Canada qui a fait la première enquête sur Facebook, mais, parallèlement, comme l'a précisé M. Boysen, les gens ici détestent les cartes d'identité. Je pense à mes électeurs qui s'insurgeraient contre cette notion.

Nous prenons Statistique Canada comme un bon exemple de la façon de ne pas faire cela. Statistique Canada a une réputation dans le monde entier et les Canadiens lui font confiance. Cette organisation pensait que ce qu'elle faisait était dans l'intérêt public, mais les Canadiens l'ont mal perçu.

Quels conseils donneriez-vous à un gouvernement qui penserait que recueillir davantage de renseignements est dans l'intérêt public? Vous avez parlé des risques éventuels qui pourraient découler d'une augmentation de l'efficacité dans la collecte, le rassemblement et le partage des données, mais vous dites qu'il nous faut des preuves pour le démontrer. Quels paramètres devrions-nous prendre en compte à cet égard?

● (1610)

M. Matthew Anthony: Beaucoup de choses sont réunies dans cette question...

Le vice-président (M. Charlie Angus): Oui.

M. Matthew Anthony: ... et je vais tenter d'y répondre.

Tout d'abord, recueillir des données, c'est comme une drogue, on s'y accoutume. C'est facile à faire. On recueille de grandes quantités de données et on ne peut pas perdre ce que l'on n'a pas. Quand je dis « Allez-y doucement », c'est que je vois des gens vivre leur plus gros cauchemar pour gérer les retombées d'une atteinte à la vie privée. Je vois ce qui arrive quand ce que j'ai conseillé de faire n'a pas été fait.

La véritable réponse à votre question se situe dans la façon d'atteindre un équilibre entre les diverses questions, soit quelles données recueillir, pourquoi les recueillir et veiller à l'obtention d'un consentement pour leur utilisation.

Le consentement d'utilisation peut être très difficile à dépister dans le cas des données historiques que l'on a déjà. Je ne pourrai pas vous dire quel consentement j'ai donné pour les données que j'ai fournies au gouvernement fédéral il y a cinq ans. Je ne m'en souviens pas et je ne pourrais pas vous le dire. Je ne me rappelle pas avoir signé une autorisation quelconque. C'était probablement caché dans les petits caractères. Le gouvernement pourrait présenter des arguments voulant que je lui aie donné un consentement, mon consentement de le faire, mais si je ne comprenais pas de quoi il s'agissait, si cela ne m'a pas été correctement communiqué, je serais alors très fâché contre vous quand vous utiliserez les données exactement comme vous aviez dit pouvoir éventuellement le faire.

Je crois que la communication et le consentement éclairé sont probablement au coeur même du cas de Statistique Canada. Cependant, je dirais: ne recueillez pas des données dont vous n'avez pas besoin, soyez très clairs dans la description de la façon dont vous les utiliserez et obtenez un consentement éclairé de la façon dont vous les utiliserez s'il s'agit de renseignements personnels.

Le vice-président (M. Charlie Angus): Merci.

Monsieur Boysen, ce que vous avez dit dans votre exemple des banques m'a interpellé. Si je n'aime pas les banques... En réalité, je traite avec ma coopérative de crédit, la Caisse populaire...

M. Andre Boysen: Cela fait partie du service.

Des députés: Oh, oh!

Le vice-président (M. Charlie Angus): ... et j'obtiens un bon service; si j'ai un problème, on m'appelle tout de suite et nous réglons le problème.

Notre comité a passé beaucoup de temps à examiner les modalités d'accès en ligne. Nous n'avons pas le choix. C'est ce que nous avons découvert au sujet de Facebook et de Google. Nous avons commencé à débattre de la question de l'antitrust, qui ne relève pas normalement de notre comité, mais pour les droits des citoyens et la protection des données... Autrement dit, si vous avez un problème avec Facebook, qu'allez-vous faire? Rien. Vous ne pouvez pas vous adresser à WhatsApp, parce qu'il est contrôlé par eux. Ils contrôlent toutes les autres voies.

En ce qui concerne l'intérêt public général, estimez-vous que le fait de n'avoir pas suffisamment de choix dans la façon dont nous accédons en ligne et la façon dont nos renseignements personnels sont recueillis et utilisés par les géants de collecte de données nuit dans l'ensemble à la cible que nous tentons d'atteindre?

M. Andre Boysen: Oui. En bref, oui, c'est un problème.

À mon avis, nous devons aborder ceci tout à fait autrement.

Le défi que nous oppose l'architecture actuelle d'Internet réside dans le fait que chaque organisation de prestation de services Web est livrée à elle-même dans la façon dont elle procède à l'inscription de ses clients en ligne. On sait ce que cela a donné pour nous tous ici dans la salle. Certains d'entre nous ont 10 mots de passe, d'autres en ont 25 et d'autres encore 100. Certains d'entre nous en ont 100, mais c'est en réalité un seul, parce que c'est le même mot de passe.

Par conséquent, dans ce modèle où tout le monde est livré à lui-même, le seul moyen d'avoir la certitude qu'une personne est réellement qui elle prétend être est l'établissement d'un processus d'adhésion très détaillé. Cela est particulièrement vrai au gouvernement, car votre obligation de diligence est extrêmement élevée. Par conséquent, il arrive souvent que le client ne puisse suivre entièrement ce processus et quand il y arrive, le fait que vous possédez toutes les données devient un problème. Par conséquent, lorsqu'il y a brèche, vous devez remédier à toutes les données.

Nous n'avons ce problème qu'en ligne. En personne, ce n'est pas vraiment un problème, parce que nous collaborons et coopérons déjà en ce qui concerne l'identité. Si je veux ouvrir un compte en banque, je présente une pièce d'identité émise par un gouvernement et quelque chose venant d'ailleurs, et j'obtiens un compte en banque. Si je veux prouver que j'ai vécu en Ontario les six derniers mois, je présente mes relevés bancaires pour démontrer que j'ai vécu à cette adresse tout ce temps-là. Nous coopérons déjà dans le monde tangible pour cette identification. Ce n'est qu'en ligne que nous avons le problème.

Je vous dirais donc, entre autres, que vous devriez envisager non seulement de régler cet aspect du point de vue du gouvernement, mais du point de vue de l'économie dans son ensemble. Si les banques sont ici aujourd'hui et souhaitent participer au mécanisme, c'est parce que de leur point de vue, ce n'est pas intéressant sur le plan du revenu. Elles souhaitent ouvrir des comptes en banque en ligne, et elles veulent faire réduire les risques. Le défi pour elles est qu'elles ne peuvent s'assurer que le permis de conduire est authentique. Les escrocs prennent une image d'un permis de conduire, effacent la photo qui s'y trouve, apposent la leur à sa place et vont en ligne obtenir une marge de crédit; les banques sont sans défense contre ce genre d'attaque.

Les banques voudraient que le gouvernement mette de l'ordre dans ses affaires et fasse en sorte que tous les documents émis par le gouvernement soient prêts à participer à l'économie numérique.

En 2008, le ministre Flaherty avait constitué un groupe de travail au Canada chargé de débattre de la façon dont les paiements numériques fonctionneraient. Ce groupe de travail a travaillé pendant deux ans. J'y ai participé et, selon le rapport produit par Pat Meredith — qui a très bien dirigé le groupe de travail —, il ne peut y avoir une économie numérique et des paiements numériques sans une identité numérique.

L'identité numérique doit pouvoir fonctionner dans l'ensemble de l'économie. Il ne s'agit pas de régler le système de soins de santé ni de régler le problème de l'ARC. Il s'agit de régler la situation pour les consommateurs dans l'ensemble de l'économie, parce que, si l'on y pense bien, le contraire signifie qu'il faut se présenter sur les lieux avec son permis de conduire pour obtenir ce que l'on veut, et cela prend beaucoup de temps.

● (1615)

Le vice-président (M. Charlie Angus): Je dois vous arrêter ici, pour que l'on puisse mettre au compte rendu que j'ai arrêté cinq secondes avant la fin de mon temps.

Des députés: Oh, oh!

Le vice-président (M. Charlie Angus): Monsieur Saini.

M. Raj Saini (Kitchener-Centre, Lib.): Je vous remercie de votre exposé.

J'aimerais tirer une chose au clair, parce que vous avez mentionné un problème chaque fois que l'on parle de carte d'identité nationale. Cependant, nous avons déjà des pièces d'identité infranationales. Nous avons un permis de conduire, un passeport et un numéro d'assurance social.

M. Andre Boysen: Oui.

M. Raj Saini: En Ontario, j'ai une carte du Régime d'assurance-maladie de l'Ontario. Il se peut que nous n'ayons pas à utiliser un seul et même numéro pour tous les éléments du système, mais notre système repose sur l'utilisation de cartes.

M. Andre Boysen: C'est exact.

M. Raj Saini: En ce qui concerne le modèle estonien, je partage votre avis. La raison pour laquelle nous utilisons cette solution, ou la raison pour laquelle nous avons commencé à l'utiliser est que l'Estonie fait partie d'un groupe de pays plus avancés que d'autres.

M. Andre Boysen: C'est vrai.

M. Raj Saini: Mais vous avez dit, et je suis tout à fait d'accord avec vous, en vérité, je crois que c'est M. Anthony qui l'a dit, l'Estonie compte 1,3 million d'habitants et une grande partie de son territoire est à l'état vierge. Le régime antérieur, lorsqu'elle était sous la coupe de la Russie, n'a pas laissé de système patrimonial. Elle dispose d'un territoire d'environ 40 000 km^2 dont la moitié est couverte de forêts. Les problèmes auxquels elle doit faire face ne se comparent en rien aux nôtres.

Il faudra toutefois que, un jour, nous adoptions une forme d'identificateur numérique. Si je vous pose cette question, M. Boysen, c'est parce que je connais votre société. J'ai lu un communiqué de presse de mars 2017 dans lequel vous dites qu'IBM et SecureKey collaborent à la mise au point d'une nouvelle identité numérique et d'un réseau de partage des attributs reposant sur la chaîne de blocs d'IBM.

Je n'ai aucune idée de ce que cela veut dire…

Des députés: Oh, oh!

M. Raj Saini: … ,mais cela fait bonne impression. La raison pour laquelle j'y fais allusion est que la technologie des chaînes de blocs est l'une de celles qu'on pourrait envisager d'étudier pour voir s'il y a des écarts. Vous avez parlé des cartes de crédit. Je suis un détaillant, un pharmacien pour être précis, et je sais combien il a été difficile d'obtenir des machines à cartes de crédit dans mon magasin. Il a fallu acquérir des connaissances. Nous avons eu quantité de papiers à remplir qu'il a fallu expédier au fournisseur. Est-il possible que la technologie des chaînes de blocs… Maintenant que cela fait un an que vous collaborez avec IBM, vous pouvez peut-être nous rappeler comment cette technologie est apparue. Le gouvernement pourrait-il se permettre de ne pas s'y adapter?

M. Andre Boysen: En bref, la réponse est oui. Dans le projet que nous proposons, les gouvernements, aussi bien le fédéral que les gouvernements provinciaux, jouent un rôle important. Ils doivent s'assurer de maximiser la réussite du projet. Le projet pourrait se passer d'eux, mais sa réussite sera beaucoup plus marquante s'ils y participent.

Vous avez toutefois tout à fait raison de rappeler que nous avons déjà ces documents. Nous les utilisons pour obtenir les services dont nous avons besoin. C'est ainsi que fonctionne le modèle actuel. Nous utilisons le modèle à notre disposition pour obtenir de nouveaux services auxquels nous n'avons pas encore accès ou des services que nous voulons.

C'est ainsi que les choses fonctionnent dans le monde réel. Le problème se pose uniquement lorsque nous voulons accéder à ces services en ligne, parce que les documents ne sont pas numérisés. L'une des choses que nous demandons est précisément de numériser les documents des gouvernements afin que leurs diverses entités puissent participer au projet avec les banques, les compagnies de télécommunications, les prestataires de soins de la santé, les compagnies d'assurances et les autres prestataires de services.

Pour revenir à votre question sur les chaînes de blocs, il y a un certain nombre de choses que j'entends dire à ce sujet. Je dirais que la première est que pour assurer la réussite du projet des chaînes de blocs, il vaut mieux ne pas parler de ces dernières, parce qu'on a déjà dit tant de choses à leur sujet. Quantité d'idées différentes de ce qu'elles sont et ne sont pas circulent déjà.

Ensuite, toujours au sujet des chaînes de blocs, l'un des sujets que j'aimerais aborder est celui de la protection des renseignements personnels. L'une des caractéristiques des chaînes de blocs, qui constitue aussi un avantage, est qu'elles sont immuables. Elles ne changeront jamais. La difficulté que cela pose quand on fait intervenir le Règlement général sur la protection des données est le droit à l'oubli. Imaginez que je consente à vos conditions pour utiliser vos services et que je vous dise ensuite: « Je veux que vous m'oubliiez ». La seule façon d'honorer l'entente que nous avions est d'effacer votre chaîne de blocs.

Ce serait vraiment une mauvaise idée que d'inscrire des renseignements personnels dans une chaîne de blocs. Cette forme de sagesse est maintenant devenue la norme. Cependant, ce qui est bien est de disposer de preuves d'intégrité.

Je voudrais revenir à l'exemple de la carte de crédit que je vous ai donné il y a quelques minutes. La difficulté, monsieur Saini, est que si j'apprends assez de choses sur vous aujourd'hui, je peux me substituer à vous sur Internet. L'organisme que j'essaie de tromper est sans défense, parce que je détiens toutes vos données. Je les ai trouvées sur le Web caché.

Nous n'avons pas ce problème avec le système des cartes de crédit. Avec ce système, il existe deux types de paiements. Lorsque je me rends dans un magasin et que je paye en personne, le risque de fraude est pratiquement nul pour les raisons que je vous ai données précédemment. Toutefois, lorsque je vais acheter quelque chose en ligne chez Amazon, Amazon ne peut pas voir ma carte de crédit. Cette transaction est donc plus risquée. On parle ici de « transaction en l'absence de carte ». C'est le cas aujourd'hui de toutes les transactions de commerce électronique. Les risques sont plus élevés.

Voici ce qu'il faut savoir: de nos jours, tout ce qui concerne l'identité se fait « en l'absence de cartes ». Nous ne savons absolument pas si tout ce qu'on nous dit est vrai.

● (1620)

M. Raj Saini: Donc…

M. Andre Boysen:

Je vous demande pardon, mais je vais finir de répondre à votre question sur les chaînes de blocs.

C'est pour vérifier les preuves d'intégrité que nous utilisons les chaînes de blocs. Pour nous, la chaîne de blocs est une méthode pour mettre en place une triple barrière afin de permettre à l'émetteur des données de prouver qu'il en est l'auteur et qu'il s'agit des mêmes données qu'il a fournies à l'utilisateur pour qu'il en fasse état. Le récepteur reçoit alors les données en sachant qu'elles n'ont pas été modifiées. Le consommateur peut alors avoir confiance que ces données n'ont pas été partagées indûment. C'est pour cela qu'on utilise des chaînes de blocs.

M. Raj Saini: Je vous remercie de cette précision. Je saisis son intérêt.

Mon second point est de rappeler que l'Estonie bénéficie d'un avantage, car elle n'a qu'un seul palier de gouvernement.

Ici au Canada, en tout cas dans la région d'où je viens, le Sud-Ouest de l'Ontario, il y a en vérité quatre paliers de gouvernement parce que nous avons un gouvernement régional. Dans l'état actuel des choses, nous avons donc quatre dépositaires de renseignements, soit le gouvernement fédéral, le gouvernement provincial, le gouvernement régional, qui élabore des politiques et fait d'autres choses, et les administrations municipales, responsables, par exemple, des taxes foncières. Chaque dépositaire gère les informations propres à son palier.

M. Andre Boysen: Et il vous faut une identification d'utilisateur et un mot de passe pour chacun d'eux.

M. Raj Saini: C'est exact.

Ce que je voulais dire est que lorsqu'il est question de fiscalité ou de santé, si vous devez prouver quelque chose, il faut que vous obteniez l'information de divers paliers de gouvernement.

Comment allez-vous parvenir à l'interopérabilité?

Vous n'avez pas à traiter avec un seul palier de gouvernement. Vous pouvez commencer par celui du gouvernement fédéral, mais, pour que cela fonctionne, vous allez devoir accéder à toutes les informations détenues par les divers paliers de gouvernement.

M. Andre Boysen: J'ai quelques commentaires à vous faire et, ensuite, Mme McIver aura quelque chose à ajouter.

En vérité, actuellement, chaque service élabore ses propres règles. C'est le cas des organismes que vous venez d'énumérer. Ils tiennent à continuer à le faire. Ils veulent obliger tout le monde à faire la même chose, parce qu'ils veulent pouvoir prendre leurs propres décisions d'affaires.

Toutefois, il est important de rappeler, comme vous l'avez fait, que lorsque vous parlez aux responsables canadiens des permis de conduire, ils vont vous dire que le permis de conduire n'est pas une pièce d'identité. Il atteste seulement que vous avez appris à conduire et pourtant vous ne pouvez pas accéder à n'importe quel service en ligne sans votre permis de conduire. Ce n'est pas une pièce d'identité, mais il est utilisé comme tel.

M. Charlie Angus: Il vous reste une minute.

M. Andre Boysen: Ce qui importe ici est de nous assurer de pouvoir obtenir un projet que les consommateurs de tous les secteurs de l'économie pourront utiliser.

Comme je tiens à céder la parole à Mme McIver, je vais m'en tenir là.

Mme Rene McIver: En résumé, pour ce service, nous comptons bien que tous les ministères et toutes les sources d'information faisant autorité participent à cet écosystème de façon à ce que moi, comme simple utilisatrice, lorsque j'aurai besoin d'échanger les renseignements provenant de ces sources multiples, je puisse le faire par l'intermédiaire de ce service en sachant qu'il ne recueillera aucune de ces informations pour créer ce nouveau piège à pirates centralisé qui pourrait devenir une autre cible d'attaques.

C'est l'organisme qui détient l'information qui exerce le pouvoir sur celle-ci.

M. Raj Saini: Combien de temps me reste-t-il, 20 ou 30 secondes?

Le vice-président (M. Charlie Angus): Vous disposez de 15 secondes, mais je suis tolérant ce soir.

M. Raj Saini: Très bien.

Je suis d'accord avec vous sur ce point. Il y a une chose qui me plaît dans le modèle estonien: il utilise un système X-Road, avec des silos d'information le long de la route. J'ignore si c'est une solution sécuritaire ou non d'un point de vue technologique. Je ne proposerais jamais que l'information soit conservée à un endroit où elle pourrait être attaquée, mais je crois que c'est ce que l'Estonie a fait. Elle a ce système X-Road sur lequel tous les services sont interconnectés.

Pouvez-vous nous dire ce que vous en pensez? S'agit-il du même type de projet?

M. Andre Boysen: La nature du projet est la même.

M. Raj Saini: D'accord.

Le vice-président (M. Charlie Angus): Je vous remercie.

Mme Rene McIver: Certainement.

[*Français*]

Le vice-président (M. Charlie Angus): Nous continuons avec M. Gourde pour cinq minutes.

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

Merci aux témoins d'être ici cet après-midi.

L'identifiant numérique unique semble être une avenue d'avenir. Par contre, j'aimais la position assez modérée de M. Anthony selon laquelle il faut prendre le temps de bien faire les choses, et ce, pour plusieurs raisons. Tout d'abord, nous avons déjà une infrastructure de services numériques offerts aux Canadiens, contrairement à l'Estonie, qui est partie de rien pour se rendre à l'identifiant numérique unique. Cependant, il ne faut pas jeter le bébé avec l'eau du bain.

Nous avons déjà investi énormément d'argent pour mettre en place des infrastructures numériques. Serons-nous obligés de les laisser tomber pour les remplacer graduellement par l'identifiant unique, ou serons-nous capables de récupérer la base de l'infrastructure existante? Si nous devons recommencer à zéro, il faudra dépenser des milliards de dollars. A-t-on une idée de l'ampleur du défi que représente ce service qu'on veut offrir à tous les Canadiens partout au pays?

Mes questions s'adressent à tous. Je ne sais pas qui veut y répondre en premier.

● (1625)

[*Traduction*]

M. Matthew Anthony: Je n'ai pas de problème à répondre à cette question ou, du moins, à contribuer à y répondre. Je ne sais pas si c'est au secteur public ou au secteur privé qu'il incombe de créer un identificateur numérique unique. Je sais, par contre, que quand j'entends parler de concepts impliquant l'emploi de mon identificateur à la banque, ou peut-être d'un autre identificateur, je veux mieux comprendre de quoi il s'agit. J'ai tendance à croire que nos institutions publiques peuvent disposer de plus d'informations qui sont davantage fiables, et qu'elles pourraient s'occuper de cette question. Mais il faut être conscient de l'ampleur de la tâche: énorme!

Je commencerai par suggérer au gouvernement fédéral d'au moins examiner l'ensemble des différents identificateurs qui sont utilisés actuellement et de choisir des endroits où il pourrait les intégrer à un système d'identification unique qui garantirait une identification de haute qualité pour les transactions qui se font au sein des services gouvernementaux et dans leur environnement. C'est par là que je commencerai avant de m'attaquer à l'extérieur.

C'est un projet d'une ampleur énorme, et je ne peux que me souvenir des commentaires de M. Boyson voulant que nous ayons un bon identificateur matériel et que le problème se pose uniquement en ligne. Je prétendrai que l'ensemble très fragile des identificateurs qui s'agrègent dans un passeport ou dans un permis de conduire ne constituent pas en vérité des authentifications rigoureuses. On ne dispose aujourd'hui que de très peu de preuves confirmant que je suis qui je dis être. J'existe, mais il n'y en a que très peu de preuves.

M. Andre Boysen: Je veux seulement ajouter qu'il ne s'agit pas d'avoir un identificateur unique, mais bien d'avoir confiance dans l'identité de la personne à l'autre bout de la transaction. Je possède déjà aujourd'hui, dans ma vraie vie, quantité d'identificateurs. L'avantage est que cela me permet de segmenter et de compartimenter ma vie afin de ne partager que certaines informations avec cet organisme et certaines autres avec d'autres.

Un identificateur unique permettrait à quelqu'un de voir tous les endroits où je suis allé sur Internet. L'entente que nous avons avec le gouvernement du Canada est que la demande formulée au départ visait à accéder à un service précis utilisant un identificateur unique. Vous vouliez un service avec un numéro unique non significatif, un MBUN, que je pourrais utiliser partout au gouvernement. Quand nous avons examiné cette solution, nous avons conclu qu'il s'agissait là d'une idée abominable parce que nous allions mettre en place un vrai réseau de surveillance. Vous pourrez savoir tous les endroits où des gens sont allés: au magasin de bière, chez le médecin, au centre fiscal. Vous auriez pu me suivre partout. Je ne veux pas de cela. Nous avons conçu un système de protection des renseignements personnels à triple barrière pour résoudre ce problème. Nous ne l'avons pas fait pour obtenir un identificateur unique. Au gouvernement, le service que nous élaborons actuellement vous donne une pluralité d'identificateurs.

Lorsque je veux accéder au service d'un ministère donné, je dispose d'un identificateur unique que je n'utilise que pour ce ministère et c'est un meilleur modèle parce que ma relation est contextuelle. Je n'ai pas une vision complète de l'ensemble de mes données. J'ai une vision très contextualisée et compartimentée de ma vie et je veux que cela reste ainsi. Je ne veux pas un gros piège à pirates quelque part. Il est important de donner aux gens les outils et les moyens de faire cela.

J'aimerais cependant revenir un instant sur les commentaires de M. Anthony. Le passeport n'est pas un document d'authentification. Nous l'utilisons à des fins d'identité, pour prouver que nous sommes bien inscrits dans les répertoires du gouvernement. Permettez-moi de partager avec vous un élément vraiment important quand il est question d'identité. Lorsque vous demandez qui est une personne donnée, vous posez en réalité deux questions auxquelles il faut répondre en même temps. La première question est: « Existe-t-il bien une personne qui s'appelle Andre Boysen? » Il ne fait aucun doute que le gouvernement est l'auteur de ce dossier et que c'est lui qui en est responsable.

La seconde question à laquelle il faut répondre en même temps est: « Est-il Andre Boysen? » Si vous ne pouvez pas répondre en même temps à ces deux questions, vous ne parviendrez pas à faire un bon travail. Vous avez une authentification impressionnante qui est vraiment rigoureuse, mais si vous ne savez pas de qui il s'agit, cela n'est pas très utile. Il faut que vous soyez en mesure de faire le lien avec la personne qui l'a fait. Si vous pouvez combiner ce mécanisme avec le propre intérêt de la personne, les utilisateurs feront alors ce qui convient lorsqu'ils perdront l'accès à la pièce d'identité, ce qui signifie que l'escroc est éliminé. Une identité est composée de trois éléments qu'il faut garder isolés les uns des autres.

Le vice-président (M. Charlie Angus): Merci.

M. Andre Boysen: La première partie est la question sur l'identité: qui êtes-vous? La deuxième question vise l'authentification: êtes-vous la même personne que celle qui s'est présentée la première fois? Le troisième élément est l'autorisation: que suis-je autorisé à faire à l'intérieur de votre service?

Ce troisième domaine englobe majoritairement ce dont vous avez parlé aujourd'hui. Les deux premières questions correspondent à ce dont nous discutons: il devrait s'agir d'un service à la fois public et privé à l'échelle de l'économie. Il faut que toutes ces organisations participent.

Le vice-président (M. Charlie Angus): Très bien, merci.

Je vais céder la parole à M. Graham.

M. David de Burgh Graham (Laurentides—Labelle, Lib.): C'était une bonne réponse.

Le vice-président (M. Charlie Angus): Oui, c'était en effet une bonne réponse. C'est pourquoi je me suis montré si raisonnable.

M. David de Burgh Graham: C'est juste.

Je ne dispose pas de beaucoup de temps, aussi je vous demanderais de recourir à ce que j'appelle la « compression de données avec perte » dans vos réponses.

Des voix: Oh, oh!

M. David de Burgh Graham: Dans le monde numérique, la protection des renseignements personnels peut-elle exister sans la sécurité?

● (1630)

M. Matthew Anthony: Oui.

M. David de Burgh Graham: La protection des renseignements personnels existe sans la sécurité.

M. Matthew Anthony: Tout dépend de l'angle sous lequel vous considérez la question. Il est question de l'accès, afin qu'un dossier puisse demeurer confidentiel. On peut discuter des moyens de le sécuriser, mais dans ce cas... C'est une question assez compliquée.

En fin de compte, tous les aspects de la protection des renseignements personnels s'expriment sous la forme d'une certaine mesure de contrôle de la sécurité. Je pense que, théoriquement, la réponse est oui, mais que, concrètement, la réponse est non.

M. Ira Goldstein: Je pense que si l'on inverse cette affirmation et que l'on dit plutôt que l'on peut se doter de certaines mesures de sécurité assorties de divers niveaux de protection des renseignements personnels, ce serait davantage en phase avec ce dont nous sommes en train de discuter.

La raison pour laquelle les sociétés motivées par les revenus publicitaires sont si populaires est simple; c'est parce que ces revenus leur permettent d'améliorer leur prestation de services ou de vous vendre davantage de choses. Le gouvernement devrait s'en inspirer — en ce qui concerne, évidemment, la protection des renseignements personnels des citoyens — pour dire que le gouvernement de l'avenir se caractérisera par une prestation de services plus précise et plus ciblée, et une prestation de services pouvant être sécurisée en fonction du niveau de protection des renseignements personnels les concernant que les citoyens sont prêts à accepter.

Si on offre aux citoyens un compromis, notamment en leur affirmant que l'on peut faire beaucoup plus au gouvernement avec les renseignements dont on dispose déjà en en faisant l'analyse, à l'instar du secteur privé, et en leur demandant s'ils sont d'accord, je pense que la majorité des Canadiens répondront positivement s'ils comprennent de quoi il retourne.

M. David de Burgh Graham: Très bien.

Monsieur Anthony, lorsque vous avez commencé à répondre à la première question de Mme Fortier, vous aviez de la difficulté à entendre parce que le microphone était allumé et, par conséquent, le haut-parleur était fermé. Ce qui était à la source du problème. Ce qui me permet de faire un lien avec un point que j'aimerais soulever au sujet des interfaces non intuitives et du fait que notre plus grand problème en matière de sécurité tient à l'utilisateur. J'ai vérifié, et cela ne figure pas au compte rendu, peut-être que ce devrait y être consigné.

Qui est Kevin Mitnick, et pourriez-vous nous en parler un peu?

M. Matthew Anthony: Vous voulez que nous parlions de Kevin Mitnick?

M. David de Burgh Graham: Je pense qu'il s'agit d'un point très important. Il a piraté un nombre impressionnant de systèmes. Il ne se servait pas vraiment d'un ordinateur pour le faire, il avait plutôt recours au piratage psychologique.

M. Matthew Anthony: En effet. Dans l'industrie, il arrive que l'on évite de qualifier Kevin Mitnick de pirate informatique. Au fond, il s'agissait d'un pirate psychologique, ce qui signifie qu'il manipulait les systèmes hors ligne et les individus pour obtenir de l'information, et qu'il s'en servait ensuite pour établir des relations de confiance avec d'autres personnes et, dans une certaine mesure, avec d'autres systèmes informatiques. Il est devenu célèbre. Il a fait de la prison. Aujourd'hui, il gagne sa vie grâce à sa célébrité et pour être allé en prison.

Si l'on considère l'ensemble de l'accès aux systèmes informatiques et aux données qui y sont stockées, et la possibilité de s'y attaquer, le mouvement naturel consistera à se diriger vers ce qui demande le moins d'effort. Et ce qui demande le moins d'effort est presque toujours le facteur humain. Donc, il ne suffit pas de sécuriser les technologies, il faut aussi contribuer à sécuriser les personnes.

M. David de Burgh Graham: C'est juste.

Oui?

Mme Rene McIver: Désolée, je voulais seulement ajouter que nous devons en arriver à un point où nous pourrons rendre les données pratiquement inutilisables. Parce que, ce qui compte vraiment, c'est la validation qui vient avec les données. Par conséquent, s'il y a une attaque — qu'il s'agisse de piratage psychologique ou autre — au cours de laquelle les agresseurs s'emparent de données et tentent de quelque manière de les réintroduire dans le système, elles seront rejetées parce qu'elles ne proviennent pas d'une source validée.

Nous voulons faire en sorte que les renseignements personnels proprement dits deviennent inutiles. Laissez les attaquants s'en emparer. Pas de problème. Ils ne peuvent rien en tirer parce qu'ils sont incapables de les valider correctement.

M. David de Burgh Graham: Tout à fait.

M. Andre Boyson: C'est l'idée sous-jacente de l'identité dans les transactions avec carte. La seule personne susceptible d'avoir effectué la transaction est quelqu'un qui avait en sa possession une chose qui appartient au véritable utilisateur, et le véritable utilisateur va annuler sa carte s'il la perd.

C'est de là que viendront la confiance et l'intégrité.

M. David de Burgh Graham: Une autre faiblesse que je vois tient au traitement des données chiffrées; tôt ou tard, il faut déchiffrer ces données pour savoir quoi faire avec.

Existe-t-il un moyen de contourner cela? Est-il possible de traiter des données sans avoir à les déchiffrer? Je sais que FFE a travaillé sur la question, mais j'ignore si on a trouvé une solution.

Mme Rene McIver: Il faut tenir compte de deux facteurs pour répondre à cette question. Tout dépend de qui veut traiter les données en question.

Dans le service où il existe un réseau d'identité, il n'est pas nécessaire que le réseau voie les renseignements protégés, n'est-ce pas? Bien entendu, il doit les transmettre. Il doit les stocker temporairement jusqu'à ce que le destinataire de l'information vienne les récupérer, mais le réseau n'a pas à voir les renseignements personnels. Donc, oui, il est possible de traiter des données sans avoir à les déchiffrer.

En réalité, le chiffrement s'effectue au niveau du fournisseur. Le destinataire de l'information devrait la déchiffrer.

L'autre facteur concerne la minimisation des données. Nous devons aussi en arriver à un point où je ne transmets pas ma date de naissance pour révéler mon âge ou que j'ai atteint la majorité; je devrais plutôt transmettre la réponse validée suivante: « Oui, cette personne est âgée de plus de 19 ans. »

Ces deux facteurs réunis peuvent contribuer à la sécurité dont nous avons besoin, du point de vue de la minimisation des données et de la réduction de l'exposition des renseignements personnels.

M. David de Burgh Graham: J'aimerais...

Qu'est-ce que vous dites?

Le vice-président (M. Charlie Angus): Cinq minutes.

M. David de Burgh Graham: Mon temps est écoulé?

Le vice-président (M. Charlie Angus): Oui. Est-ce que c'est correct? Vous vous débrouillez si bien.

M. David de Burgh Graham: Il me reste encore au moins cinq minutes.

Le vice-président (M. Charlie Angus): Je sais, mais je dois les accorder à M. Kent.

L'hon. Peter Kent: C'est la dure réalité.

Monsieur Boysen, j'aimerais revenir à votre point. Le programme de cartes NEXUS utilise les données biométriques, pas dans tous les cas, mais dans certaines situations... Et parfois, le service des passeports canadiens le fait également; nous utilisons les empreintes digitales ou les images d'iris. Diriez-vous qu'il s'agit du genre d'identification positive parfaite et double dont vous nous parliez?

● (1635)

M. Andre Boysen: En effet. Ce qui me plaisait dans le programme de la carte NEXUS, c'est qu'il laissait le choix aux consommateurs. Si vous disiez aux Canadiens qu'ils doivent subir un balayage biométrique de l'iris pour obtenir un passeport, cela susciterait une vive indignation.

L'hon. Peter Kent: En effet.

M. Andre Boysen: Cependant, si vous donnez le choix aux gens en leur disant: « Si vous voulez accélérer le service dans les aéroports, il suffit de soumettre vos données biométriques, et vous franchirez les contrôles beaucoup plus rapidement ». Et beaucoup de gens ont fait ce choix. En laissant la possibilité de faire un choix, ces contraintes ont été acceptées.

J'ajouterais que votre propre service de connexion au gouvernement du Canada, le service des partenaires de connexion, lui aussi donne le choix. Vous n'avez pas forcé les Canadiens à utiliser leur compte de banque pour avoir accès à l'ARC s'ils ne le souhaitaient pas. Ils pouvaient toujours continuer d'utiliser un ID utilisateur fourni par le gouvernement et un mot de passe. En leur donnant le choix, vous les avez rassurés. Je ne suis pas forcé, donc je vais l'essayer et je verrai bien comment les choses se passent. Cet élément de choix est une composante clé dans l'adoption de systèmes comme celui-ci.

L'hon. Peter Kent: La technologie de reconnaissance de l'iris utilisée pour la carte du programme NEXUS, dont l'acquisition n'a pas encore été effectuée, semble représenter une énorme montagne à gravir pour le gouvernement, le ministre des Finances et son budget.

M. Andre Boysen: Je me permettrais de dire que ce n'est pas vraiment un bon outil pour la prestation de services en ligne. Ça me semble un peu exagéré d'exiger un balayage de la rétine si tout ce que je veux c'est me prévaloir de mon droit de vote. J'ajouterais que chacun de ces outils doit être utilisé... Il faut considérer l'ensemble des services et également, le niveau d'assurance. Toutes ces choses ne relèvent pas de la même catégorie.

En ce qui concerne les services exigeant un faible niveau d'assurance, il n'est pas nécessaire de se doter d'un tel niveau de confiance; dans ces situations, l'atteinte d'un tel niveau de fiabilité n'est pas aussi importante. Dans le cas du balayage de la rétine et de la carte du programme NEXUS, il faut également tenir compte du fait que les activités se déroulent dans un environnement contrôlé. Il faut se rendre à un poste contrôlé où des gens nous observent pour s'assurer que l'on n'essaie pas de trafiquer la machine ou de tripoter la carte. C'est cet environnement contrôlé qui est garant du processus. Vous ne pourriez pas procéder à un balayage de la rétine à partir de chez vous, par exemple, sans aucune forme de garantie, parce qu'il pourrait s'agir d'une attaque par réinsertion.

L'hon. Peter Kent: Déjà.

M. Andre Boysen: Oui, déjà.

M. Ira Goldstein: Mais peut-être pourriez-vous le faire finalement si nous nous inspirons du secteur privé et si nous examinons l'une des méthodes d'authentification les plus élégantes qui existent aujourd'hui. Avec les téléphones intelligents, les données biométriques et la reconnaissance faciale sont désormais monnaie courante. Effectuer un balayage de votre visage chaque fois que vous souhaitez déverrouiller votre téléphone peut sembler une approche indûment rigoureuse, mais vous savez quoi? Maintenant, c'est la réalité; les gens ne s'en formalisent pas parce que la technologie est tellement avancée, et qu'ils veulent y avoir accès, et que ça leur facilite les choses.

Je pense que nous devrions nous en inspirer. L'authentification est utilisée aujourd'hui de bien des manières, notamment lorsque l'on utilise les données biométriques chaque fois que l'on veut ouvrir son téléphone. Et il ne s'agit pas d'un nouveau système, mais d'un système existant, qui est déjà en place.

M. Andre Boysen: Permettez-moi d'ajouter des précisions, l'utilisation des données biométriques sur un appareil est une bonne idée. Mais essayer d'enregistrer ses données biométriques à droite et à gauche n'est pas une bonne idée. C'est l'argument que j'essayais de faire valoir.

L'hon. Peter Kent: À Toronto, les hôpitaux, les réseaux d'hôpitaux tentent depuis plus d'une décennie de... Le gouvernement de l'Ontario les encourage à mettre en place un système d'échange en ligne de renseignements d'ordre médical pour un éventail de raisons — accès à l'urgence et ainsi de suite.

Est-ce que l'une ou l'autre de vos entreprises a travaillé avec les réseaux d'hôpitaux, les cabinets de médecins pour tenter de parvenir à un système sûr?

M. Andre Boysen: Oui, nous avons actuellement un projet pilote en cours avec le Réseau universitaire de santé. L'une des difficultés que... et j'ai d'ailleurs présenté un exposé TED sur les soins de santé et l'identité, parce que, à l'échelle du pays, le besoin le plus important en matière d'identité numérique se trouve dans les soins de santé. Nous devons résoudre ce problème parce que nous ne pouvons pas continuer à laisser les soins de santé gruger le budget.

Nous menons des projets pilotes actuellement. L'un des éléments cruciaux pour redresser la situation dans les soins de santé est qu'une solution sur mesure visant les « soins de santé seulement » ne fonctionnera pas. La raison en est que la majorité de la population utilise le système de soins de santé très rarement, ce qui signifie que les gens vont finir par oublier leur fichu mot de passe. Quant au reste de la population, il est constitué d'utilisateurs très assidus du système de santé qui, de toute façon, se rendent toujours sur place.

Il nous faut un mécanisme d'accès aux services en ligne qui fonctionnera pour les Canadiens ordinaires. Nous avons vu à quel point le service gouvernemental a donné de bons résultats pour l'ARC. C'est pourquoi nous pensons que ce modèle pourrait être étendu à d'autres services des secteurs public et privé.

Le vice-président (M. Charlie Angus): Il s'agit cette fois du dernier tour.

C'est M. Saini qui commence.

M. Raj Saini: J'ai une question rapide. Si vous ne pouvez pas me fournir une réponse complète aujourd'hui, pourriez-vous le faire ultérieurement par écrit? Je l'apprécierais beaucoup.

Nous parlons de l'Estonie, mais je sais que d'autres pays ont amorcé le processus. Si vous pouviez nous fournir la liste de ces pays ou nous suggérer une liste de pays que nous devrions étudier, et peut-être de la documentation pertinente, nous pourrions nous en servir dans le cadre de notre étude.

Et ensuite, voilà une chose qui me fascine, parce que, étant issu du secteur privé, et propriétaire d'une pharmacie, ma technologie était toujours à la fine pointe. Peu importe ce qu'il y avait de plus récent, je devais emboîter le pas. Maintenant, il est question d'un point NEXUS qui ira de l'avant, et dans ce contexte, le secteur privé et le secteur public vont échanger de l'information.

Comment faire pour que la technologie demeure à jour parce que le secteur privé sera toujours en avance? Le secteur public tire de l'arrière. Peu importe si les directives en matière de politique sont justes, si tout le monde a bien compris, on peut régler les problèmes en lien avec la protection des renseignements personnels, mais tôt ou tard la technologie deviendra l'élément clé parce que l'une des deux parties sera toujours en décalage avec l'autre. Si nous voulons que tout cela fonctionne correctement, comment devrions-nous procéder pour régler ce problème?

M. Andre Boysen: J'aimerais revenir sur le commentaire de Matthew tout à l'heure, comme quoi il faut procéder lentement parfois, et ensuite rapidement, lorsque c'est possible.

Si on compare Internet et le système de paiement par carte, il est intéressant de souligner que notre manière de régler nos achats a à peine changé depuis 70 ans. Au début, nous avions une carte en papier, puis plus tard elle a été remplacée par une carte en plastique. Ensuite, nous avons fait face à deux problèmes, la vitesse des transactions et la fraude, alors nous sommes passés à la bande magnétique. Puis les escrocs ont compris comment fonctionnait la bande magnétique, et c'est alors que nous sommes passés à la carte à puce. Depuis l'adoption de la carte à puce, la fraude en personne est devenue quasi nulle, mais il reste le problème des transactions en ligne, c'est pourquoi maintenant nous la mettons dans le téléphone.

Ce qui importe, c'est que la manière dont les acheteurs paient leurs achats partout dans le monde a à peine changé en 70 ans. Sur Internet, ce mode de paiement change pratiquement toutes les semaines. Les utilisateurs ont du mal à suivre.

● (1640)

M. David de Burgh Graham: Vous parliez tout à l'heure de la reconnaissance faciale pour l'ouverture de session ou la connexion.

Si vos données biométriques ont été compromises, que pouvez-vous y faire? J'en prends pour exemple le célèbre cas du piratage des empreintes digitales d'Angela Merkel à partir d'une photographie de cette dernière.

M. Ira Goldstein: J'aimerais vous reporter à mon exemple de l'assurance-dépôts pour vous dire que, si nous décidons d'y aller avec le déploiement de l'authentification à l'aide de données biométriques dans le contexte des services gouvernementaux, il faudra prévoir une zone tampon grâce à laquelle les citoyens seront persuadés qu'en cas de compromission, il y aura toujours un moyen de corriger le problème.

Comment faut-il faire pour obtenir de nouvelles données biométriques? Je n'ai malheureusement pas de bonne réponse à cette question. Peut-être que Matt peut répondre.

M. Matthew Anthony: D'entrée de jeu, je dirais qu'il devient de plus en plus difficile de falsifier des données biométriques compte tenu de la sophistication de la technologie des capteurs. Par conséquent, alors que nous délaissons les empreintes digitales pour les images du visage — il est même question d'utiliser la reconnaissance du réseau veineux sur certains nouveaux systèmes téléphoniques... Nous avons utilisé la technologie de l'empreinte palmaire pendant longtemps. Peut-être qu'il est toujours possible de créer quelque mystification avec ces données. N'importe quel problème peut être résolu si on y consacre suffisamment de temps et la technologie nécessaire. On peut les trafiquer, mais je doute que l'on puisse les usurper, à moins que vous ne les ayez pas enregistrées vous-même.

Je m'explique. Si vous possédez un téléphone et que vous n'enregistrez rien, sauf un NIP à quatre chiffres, et qu'une personne s'empare de votre téléphone et y enregistre l'empreinte de son pouce, c'est trop tard, son empreinte est enregistrée dans votre appareil. Cela vous incombe, et pas à eux. La capacité de se faire passer pour quelqu'un d'autre à l'aide de données biométriques, à moins que vous n'ayez enregistré les vôtres au départ, est en train de devenir pratiquement impossible. Il y a 15 ans, je pouvais falsifier une empreinte digitale, et la réexécuter assez facilement. Mais désormais ce n'est plus possible.

M. David de Burgh Graham: Je comprends.

Mme Rene McIver: Tout tourne autour de la manière dont elles sont entrées dans le système, encore une fois. J'ai travaillé sur les normes relatives aux données biométriques pendant près de 10 ans en fait, et c'était intéressant. Il y avait toujours une discussion au sujet de l'entrée dans le système et de la prise de l'empreinte et de l'insertion de l'empreinte. Il y avait toujours une discussion au sujet de la détection du caractère vivant. Mais dans les faits, le système d'entrée doit comporter un moyen de détecter s'il s'agit vraiment de données biométriques réelles. Le caractère vivant caractérise vraiment les données biométriques; il devient donc de plus en plus complexe de trouver comment obtenir avec précision l'information qui prouve qu'elle n'a pas été trafiquée. Il ne s'agit pas seulement d'une empreinte digitale statique.

On peut voir la même chose dans les algorithmes de reconnaissance faciale. L'entrée des données passe par une requête vous demandant d'exécuter diverses choses, comme sourire, tourner la tête, regarder vers le bas ou fermer les yeux. Il devient de plus en plus difficile de mettre la main sur les données saisies.

M. Matthew Anthony: Si je peux me permettre, j'ajouterais simplement que si le niveau d'accès dont vous avez besoin exige de telles précautions, je vous garantis qu'il existe des moyens plus simples d'obtenir vos données.

M. David de Burgh Graham: Je comprends.

M. Andre Boysen: Je ne veux pas prendre trop de votre temps, mais j'aimerais ajouter qu'en ce qui concerne les données biométriques, il ne faut pas les voir comme une solution miracle, et s'imaginer que l'on va régler tous les problèmes grâce à elles. Il faut plutôt penser à l'utilisation des données biométriques avec ce que vous avez déjà, et ce que vous n'avez pas.

Le vice-président (M. Charlie Angus): Merci beaucoup.

J'ai vraiment l'impression que mon collègue M. Graham se lancerait dans l'obstruction, s'il le pouvait, parce qu'il a vraiment beaucoup de choses à dire. Normalement, j'aimerais bien poursuivre, mais comme nous avons pris l'engagement de finir tôt les jeudis, afin d'accommoder ceux qui ont des vols à prendre, nous allons mettre fin à la séance après cette série de questions.

Je vous remercie énormément. Nous avons eu une discussion fascinante et obtenu d'excellents renseignements. Si vous pensez à des éléments d'information susceptibles de nous être utiles dans notre étude ou si vous consultez nos témoignages à ce sujet, n'hésitez pas à nous faire part de vos commentaires parce que nous allons préparer un rapport.

Je vous en prie, monsieur Saini.

M. Raj Saini: Je m'adresse à vous quatre, j'ai mentionné la question au sujet des pays, mais si vous pensez à tout autre renseignement susceptible de nous aider, nous vous serions très reconnaissants de nous le transmettre dans une déclaration pour que nous ayons la possibilité d'élargir notre réflexion sur ce sujet.

M. Andre Boysen: Nous vous transmettrons de l'information, soyez-en sûrs.

Merci de nous avoir invités.

Le vice-président (M. Charlie Angus): La séance est levée.