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 023 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mardi 20 septembre 2016

Président

M. Blaine Calkins

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

Le mardi 20 septembre 2016

● (1105)

[*Traduction*]

Le président (M. Blaine Calkins (Red Deer—Lacombe, PCC)): Mesdames et messieurs, je déclare la séance ouverte. Nous accusons un léger retard en raison des problèmes éprouvés par le comité précédent.

J'aimerais vous souhaiter à tous un bon retour. Quelle joie de voir des visages heureux et souriants, et de constater que tout le monde est de retour de vacances en bonne santé. J'espère que vous avez tous eu le meilleur été possible.

Nous allons reprendre notre étude de la Loi sur la protection des renseignements personnels. Nous avons le plaisir de recevoir aujourd'hui quatre témoins que je serai heureux de vous présenter dans un instant.

Je tiens à vous informer que j'ai réservé une quinzaine de minutes à la fin de la séance pour nous permettre de revoir les questions figurant à notre programme et en discuter, et de faire un peu de planification. Comme aucun témoin n'est prévu jeudi, je voudrais utiliser le temps réservé à la fin de la présente séance pour discuter du déroulement du reste de notre étude et de ce que nous entreprendrons ensuite.

Nous avons un nouveau greffier, qui s'appelle Hugues La Rue, je pense.

Le greffier du comité (M. Hugues La Rue): Bonjour.

Le président: Voilà pour les présentations.

Nous vous souhaitons la bienvenue parmi nous. Merci beaucoup d'avoir tout préparé à notre intention.

Mesdames et messieurs, un de nos témoins comparaît par vidéoconférence. C'est avec plaisir que nous entendrons Brenda McPhail, directrice, Confidentialité, technologie et surveillance, de l'Association canadienne des libertés civiles.

M'entendez-vous bien?

Mme Brenda McPhail (directrice, Confidentialité, technologie et surveillance, Association canadienne des libertés civiles): Oui, merci.

Le président: Formidable.

Nous recevons également Tom Keenan, professeur de l'Université de Calgary, Ken Rubin, que nous connaissons déjà et qui nous revient pour traiter de la Loi sur la protection des renseignements personnels, et Tamir Israel, avocat à la Clinique d'intérêt public et de politique d'internet du Canada Samuelson-Glushko, qui témoigneront à titre personnel.

J'avise les témoins que nous leur accordons une dizaine de minutes pour faire un exposé. Nous vous prions de respecter le temps qui vous est alloué. Vous n'êtes pas obligés de l'utiliser au complet. Les députés vous interrogeront ensuite, ce qui nous mènera à 12 h 45 environ. Espérons que nous aurons fait le tour de la question à ce moment-là.

Nous allons simplement suivre l'ordre figurant dans l'ordre du jour. Brenda, êtes-vous prête à faire votre exposé?

Mme Brenda McPhail: Oui, merci.

Je vous remercie de permettre à l'Association canadienne des libertés civiles de comparaître aujourd'hui devant le Comité.

L'Association a été fondée en 1964 pour protéger les droits et libertés chers au coeur des Canadiens et enchâssés dans la Constitution.

De nos jours, la protection des renseignements personnels est trop souvent considérée comme une barrière que l'on peut décider d'ériger ou d'abattre. Un établissement ou un groupe peut vouloir l'élever, l'abaisser ou la réduire à néant, selon la valeur qu'il accorde à la protection des renseignements personnels. La métaphore de la barrière, que l'on voit de plus en plus dans les médias et d'autres discussions au sujet du chiffrement, des renseignements sur la santé et de la sécurité nationale — pour ne nommer que ces domaines —, est une façon improductive, porteuse de conflits et, selon d'aucuns, inefficace de réfléchir à la protection des renseignements personnels et d'en parler.

Selon l'ACLC, il faut parler de la protection des renseignements personnels comme d'un droit de la personne, particulièrement dans le cadre de la présente discussion sur la loi fédérale du Canada en la matière, discussion qui ne s'est que trop fait attendre. Une approche fondée sur les droits n'élimine évidemment pas tous les problèmes, car tout droit protégé par la Charte ou enchâssé dans le droit international peut entrer en conflit avec d'autres droits. Cette approche nous incite cependant à agir en vertu de principes premiers. Ainsi, lorsque l'on commence à préciser en quoi consiste la protection des renseignements personnels au Canada, on s'appuie tous sur une compréhension commune de la question, pas seulement à titre de particuliers, mais en tant que société, et ce, à l'échelle tant nationale qu'internationale. Le fait de considérer la protection des renseignements personnels comme un droit de la personne peut nous aider à composer avec les changements dramatiques auxquels nous avons assisté depuis que la loi est entrée en vigueur il y a 30 ans.

La technologie a modifié non seulement la manière dont nous pouvons recueillir et utiliser les renseignements, mais aussi l'attitude de notre société à l'égard de l'information. Les organismes sectoriels privés et publics font régulièrement miroiter la possibilité de recueillir des sommes considérables de renseignements — les mégadonnées — afin de déceler des tendances utiles et probablement des secrets cachés. Le gouvernement lui-même recueille des renseignements et a potentiellement accès aux banques d'informations en constante croissance du secteur privé. Cependant, selon ce que nous disent les gens qui communiquent avec l'ACLC, les citoyens craignent que des technologies et des processus qu'ils ne comprennent pas soient utilisés à leur insu de manières qui pourraient avoir de lourdes conséquences sur leur vie. Cette crainte légitime mine la confiance de la population à l'égard des organismes, y compris les gouvernements, qui recueillent, gèrent et entreposent les renseignements.

Dans ce contexte d'abondance de données rempli d'acteurs assoiffés de données et de citoyens craintifs, il importe de plus en plus de réviser la loi canadienne sur la protection des renseignements personnels pour qu'elle soit solide, souple et bien fondée. Elle doit englober les utilisations actuelles et futures des renseignements personnels et, surtout, engendrer la confiance chez les Canadiens.

Nous avons formulé toutes nos recommandations avec ces grandes préoccupations à l'esprit. Je vais passer rapidement en revue 10 points, dont la plupart vous seront familiers, car ils cadrent avec ceux que le commissaire à la protection de la vie privée du Canada et des témoins subséquents vous ont présentés en mars dernier. Je vais être extrêmement brève, mais je me ferai un plaisir d'apporter des éclaircissements au cours de la période de questions.

Nous devons d'abord veiller à ce que la loi comprenne une norme relative à la nécessité et à la rectitude, laquelle s'appliquerait lorsque l'on décide s'il faut recueillir, conserver et communiquer des renseignements. Est-ce nécessaire de le faire? Convient-il de recueillir et d'utiliser les renseignements? J'entends par là qu'il faut se demander si cette collecte et cette utilisation résisteraient à une contestation en vertu de la Charte. Cette norme favorisera une réduction de la somme de données colligées et préviendra la tendance, bien connue de tous, à recueillir trop de données et à les conserver trop longtemps, juste au cas où elles pourraient être utiles dans l'avenir.

Il faut également clarifier les exigences relatives aux ententes sur l'échange de renseignements dans la loi. C'est particulièrement crucial depuis l'adoption de la Loi antiterroriste, en 2015, laquelle a considérablement élargi l'ampleur de l'échange de renseignements entre les ministères. À l'époque où le projet de loi C-51 a été adopté, on a assuré à la population canadienne, à propos de ces nouveaux pouvoirs d'échange de renseignements, que le Commissariat à la protection de la vie privée du Canada en effectuerait l'examen et la supervision. Sans égard aux changements qui seront apportés ou non à la suite de la consultation réalisée actuellement en matière de sécurité nationale, nous considérons que les modifications faites à la Loi sur la protection des renseignements personnels peuvent prévoir des mesures de précaution et de transparence fort nécessaires pour tous les renseignements et toutes les fins au Canada. Il faut faire preuve d'ouverture et de transparence quant à la manière dont les renseignements sont échangés, à l'ampleur de cet échange et aux mesures de précaution explicites qui, présumons-nous, seront instaurées pour veiller à ce que l'échange soit proportionnel et que les risques relatifs à la protection de la vie privée aient été adéquatement évalués et atténués. Bien entendu, cela s'applique à l'échange de renseignements au pays et avec les gouvernements étrangers.

Dans la même veine, des exigences en matière de rapports de transparence doivent être éclaircies et établies. C'est notamment le cas pour les demandes d'accès légal présentées dans le cadre de l'exécution de la loi aux organismes du secteur privé qui détiennent des renseignements sur des citoyens. Ces rapports fournissent de précieux renseignements publics qui peuvent favoriser et éclairer les débats et les décisions publics sur la protection des renseignements personnels et, pour en revenir à ce que j'ai dit plus tôt, renforcer la confiance à l'égard des institutions gouvernementales. Les citoyens méritent de comprendre la nature et la fréquence des demandes que présentent les organismes d'exécution de la loi pour obtenir leurs renseignements personnels lorsqu'ils le font sans leur consentement et à leur insu; bien souvent, ils veulent comprendre. L'ACLC a toujours affirmé que la capacité des organismes d'exécution de la loi de faire telles demandes devrait être restreinte, conformément à l'arrêt *Spencer*, mais dans la mesure où ces demandes sont autorisées, avec ou sans mandat, un solide régime de transparence s'impose pour que le public soit convenablement informé.

Toujours sous le thème du renforcement de la confiance de la population à l'égard de la manière dont le gouvernement recueille et utilise les renseignements personnels, l'ACLC recommanderait également que des évaluations des facteurs relatifs à la vie privée soient obligatoires lorsque des ministères créent ou élargissent des programmes qui pourraient avoir des répercussions sur la protection des renseignements personnels. Ces évaluations doivent être remises au Commissariat à la protection de la vie privée, qui les examinera à l'étape de conception et de planification, alors qu'il est encore temps d'atténuer les risques relatifs à la protection des renseignements personnels. Une fois le processus terminé, des résumés appropriés devraient être publiés pour que les citoyens puissent constater que ce processus a eu lieu.

● (1110)

De même, nous proposons de consulter le CPVP lors de l'élaboration de lois et de règlements qui ont des répercussions sur la protection des renseignements personnels des Canadiens. Ici encore, cette consultation devrait avoir lieu avant le dépôt des projets de loi. Cette recommandation a un lien direct avec mon préambule, au cours duquel j'ai préconisé que l'on considère la protection des renseignements personnels comme un droit de la personne. Le fait de disposer d'un processus permettant de démontrer que les intérêts relatifs à la protection des renseignements personnels ont été pris en compte au cours de l'élaboration d'une nouvelle loi confère aux droits au respect de la vie privée un poids approprié et cadre avec les tendances internationales.

Nous encouragerions aussi les institutions gouvernementales à faire figure d'exemple au chapitre de la cybersécurité grâce à l'ajout d'une exigence précise dans la loi les obligeant à assurer le niveau approprié de protection technologique et procédurale des renseignements qu'elles recueillent, que ce soit lors de leur communication, de leur conservation, de leur utilisation, de leur entreposage ou de leur destruction. Nous recommandons que le gouvernement fédéral adopte une approche proactive pour assurer la protection des renseignements que détiennent ses institutions en vertu d'une norme exemplaire. Nous considérons qu'il peut notamment y parvenir en modifiant la Loi sur la protection des renseignements personnels. Bien entendu, l'examen de la cybersécurité permettra d'obtenir plus d'informations à ce sujet.

Nous voudrions aussi que le signalement des atteintes à la vie privée soit obligatoire dans la loi plutôt que dans les politiques. Les institutions gouvernementales devraient devoir signaler ces atteintes au CPVP au-delà d'un seuil pertinent et convenu, et aviser les personnes concernées sans tarder. Il faut préciser clairement ce seuil dans la loi, comme on l'a fait lors de la modification de la LPRPDE.

Même si les atteintes sont inférieures au seuil convenu aux fins de signalement, les institutions gouvernementales devraient être tenues de conserver un registre de toutes les atteintes en vue d'un examen possible de la part du CPVP. Le fait de savoir qu'elles y sont obligées les incitera fortement à assurer la sécurité nécessaire des renseignements et à améliorer la gérance des données.

Les exigences en matière de tenue de registre doivent être suffisamment strictes pour que le commissaire puisse examiner les atteintes afin de s'assurer que l'on évalue correctement si elles correspondent ou non au seuil.

Nous voudrions également que le commissaire à la protection de la vie privée se voie conférer un pouvoir de prise de décret. Nous avons remarqué avec intérêt qu'il est maintenant d'accord. Plus il s'échange et se recueille de renseignements, plus les excès peuvent causer de torts. Les conséquences doivent être proportionnelles aux risques; le commissaire a donc besoin de pouvoirs élargis pour assurer l'application efficace et en temps opportun de la protection accrue prévue dans la loi révisée.

Nous recommandons enfin un examen régulier de la loi, tous les cinq ans. Je pense que cette recommandation se passe d'explication dans l'environnement changeant actuel.

Je vous remercie une fois de plus de nous avoir permis de témoigner.

● (1115)

Le président: Merci beaucoup, madame McPhail.

Nous entendrons maintenant M. Keenan, pour 10 minutes.

M. Thomas Keenan (professeur, University of Calgary, à titre personnel): Merci beaucoup, monsieur le président, de m'avoir invité à participer à votre séance. Je vais vous faire part de certaines de mes réflexions à propos des technologies qui sont sur le point d'être lancées et qui, selon moi, auront une incidence notable sur la manière dont nous considérons la protection des renseignements personnels. Ce que je veux, c'est nous aider à mieux les comprendre pour que nos lois soient le plus prêtes possible pour ce qui nous attend.

Je suis professeur à la faculté de design de l'environnement de l'Université de Calgary, ainsi que professeur auxiliaire en informatique. Je suis également chercheur universitaire au Centre for Military, Security and Strategic Studies et à l'Institut canadien des affaires mondiales, ici, à Ottawa. J'ai pris la parole à toutes les grandes conférences sur le piratage, comme DEF CON, Black Hat et une qui porte le nom intriguant de Hackers on Planet Earth. J'essaie donc de me tenir au courant des activités des bons et des mauvais pirates.

Je suis aussi pas mal certain d'avoir donné le premier cours sur la sécurité de l'information au Canada, en 1974. Les choses étaient simples à l'époque: barrez les portes des locaux où se trouvent les ordinateurs, choisissez un bon mot de passe et ne mettez pas de documents confidentiels dans les poubelles. La situation est plus complexe aujourd'hui.

Pensez à un projet appelé « The Face of Litter », réalisé en 2015 sous l'égide de Hong Kong Cleanup. Des employés ont ramassé des gommes et des mégots de cigarette jetés dans les rues de la ville et les ont envoyés à Parabon NanoLabs, une société privée du Delaware. Cette dernière a procédé à la détermination du phénotype grâce à l'ADN afin de créer un portait numérique approximatif à partir de chaque échantillon. Une semaine plus tard, en passant sur les lieux du crime, le coupable pouvait voir un visage étrangement familier sur un écran vidéo: son propre portrait établi au moyen de son ADN.

Mais comment a-t-on pu réaliser ce portrait? Il restait amplement de salive sur les gommes et les mégots pour effectuer une analyse de l'ADN. En fait, il n'en faut qu'un nanogramme. Certains traits, comme la couleur des yeux et des cheveux et la forme du visage, peuvent être aisément déterminés. L'ascendance peut être analysée. Ajoutez à cela l'intelligence artificielle et la connaissance du monde réel — les mâcheurs de gomme sont plus susceptibles d'être âgés de 18 à 34 ans, alors que les fumeurs sont plus âgés — et on se retrouve dans un scénario inquiétant où les données biographiques sont utilisées non pas pour identifier une personne en particulier, mais pour faire des suppositions à son sujet. Voilà qui remet en question nos vieilles définitions de renseignements permettant d'identifier une personne et de renseignements personnels sur la santé.

Dans le livre intitulé *Technocreep: The Surrender of Privacy and the Capitalization of Intimacy* que j'ai publié en 2014, je laisse entendre qu'un magasin pourrait mettre la main sur quelques cellules de peau quand nous tapez votre NIP et les envoyer pour les faire analyser. À votre prochaine visite à ce magasin, vous pourriez voir une annonce vous demandant si vous êtes prédiabétique et vous proposant un coupon spécial. Même si, à ce que je sache, aucun magasin n'a encore agi de la sorte, certains commerces de détail des États-Unis et du Royaume-Uni recourent à la reconnaissance faciale pour identifier les voleurs à l'étalage, les clients de marque et les personnes dont on sait qu'elles causent des problèmes. Des banques, comme la HSBC, utilisent déjà la reconnaissance faciale pour identifier les clients, et plusieurs banques canadiennes procèdent à des essais biométriques.

Or, les définitions de renseignements personnels sur la santé de la Loi sur la protection des renseignements personnels et de la LPRPDE pourraient bien englober les données biométriques, qu'il s'agisse de la voix, du visage ou de l'ADN, même s'il faudra adapter ces définitions à mesure que les technologies évoluent. Mais cette protection juridique aide-t-elle le citoyen moyen? Dans les faits, bien des clients ne remarqueront pas une obscure disposition autorisant l'utilisation de leurs données biométriques dans les secteurs du commerce au détail ou des banques. Cette disposition pourrait être camouflée dans les conditions du document, que pratiquement personne ne lit. Certains pourraient même accorder leur consentement dans l'espoir d'économiser de l'argent, de recevoir un meilleur service ou d'obtenir des renseignements utiles sur la santé.

Je pense que les citoyens ne comprennent peut-être pas parfaitement toutes les implications de la collecte, de l'entreposage et de l'échange de leurs données biométriques, ainsi que les utilisations secondaires et la corrélation croisée des données biométriques et d'autres bases de données. Il faut que les lois exigent la divulgation pleine et entière et prévoient un processus pour assurer une véritable observation. Il faut donc plus que des lignes directrices publiées sur le site du CPVP. Même aujourd'hui, les caméras de surveillance publique visibles sont censées être accompagnées d'une pancarte claire, mais d'après mon expérience, la plupart n'en ont pas et personne n'intervient.

Le temps pose également un problème. Il y a 50 ans, un criminel aurait pu laisser impunément du sang sur une scène de crime puisque ce sang ne fournissait pas beaucoup d'information à part le groupe sanguin. De nos jours, les organismes d'exécution de la loi résolvent des affaires non résolues mises de côté depuis longtemps grâce à l'analyse de l'ADN de vieux échantillons.

● (1120)

On ne peut pas prédire les données que pourront extraire les analystes, à l'avenir, à partir de nos données biologiques et biométriques, mais une chose est sûre, ils pourront en recueillir plus qu'aujourd'hui. Les experts croient également que les ordinateurs quantiques seront en mesure de décrypter de façon rétroactive des décennies de données qui nous semblent sûres pour l'instant. Il faut donc faire très attention aux robots de l'avenir qui pourront voyager dans le temps.

Je constate que c'est un sujet qui inquiète de plus en plus les Canadiens. Lorsque j'aborde la question des identificateurs biométriques, que ce soit la forme de l'oreille, le rythme cardiaque ou l'odeur corporelle, bref tout ce qui peut vous identifier, tout le monde prête l'oreille. Récemment, j'ai été pressenti par le magazine de Costco pour rédiger un article sur les inconvénients de l'identification biométrique. J'ai expliqué comment les empreintes digitales pouvaient être volées puis falsifiées à l'aide d'une imprimante 3-D. Un pirate informatique nommé Starbug a même prélevé les empreintes digitales de la ministre de la Défense allemande à partir d'une photo à haute résolution de sa main.

Ce qui est encore plus troublant, c'est qu'on croit que les données biométriques sont infaillibles, ce qui n'est pas le cas. Le taux d'erreur dépend des paramètres établis par les concepteurs. Les terminaux NEXUS de première génération utilisés aux frontières canadiennes n'obtiendraient pas toujours des résultats en se fondant uniquement sur la biométrie oculaire.

L'Illinois et le Texas ont adopté des lois précises sur l'utilisation des données obtenues par la biométrie à des fins commerciales, et le paragraphe 9(1) du projet de règlement général sur la protection des données de l'Union européenne impose des restrictions sur l'utilisation des données génétiques et biométriques lorsqu'elles sont traitées pour identifier une personne de façon unique. Les Canadiens ont besoin d'un niveau semblable de protection, et ces lois nous donnent un point de départ.

Un autre domaine auquel il faut réfléchir sérieusement est la biométrie comportementale. Dans *Technocreep*, je m'intéresse au dispositif Snapshot de l'assurance Progressive, que les gens installent volontairement dans leur voiture pour essayer de faire baisser leurs primes d'assurance. Cet appareil recueille des données sur la conduite des gens, notamment la fréquence de conduite et l'utilisation des freins. Selon moi, cela pourrait être un choix sensé pour certaines personnes, étant donné qu'il n'enregistre pas leurs déplacements. Il y a aussi Desjardins qui peut maintenant suivre et évaluer vos habitudes de conduite à partir de votre téléphone intelligent grâce à sa nouvelle application Ajusto. Contrairement à Snapshot, ce système sait exactement où vous êtes et même dans quelle mesure vous respectez les limites de vitesse.

À l'heure actuelle, ce type de systèmes est facultatif, et les compagnies d'assurances s'efforcent de dire à leurs clients qu'ils ne verront jamais leur prime augmentée en raison d'une mauvaise conduite. Cependant, il est probable que ces dispositifs de surveillance portatifs deviennent obligatoires de facto pour obtenir une assurance à un taux raisonnable. Après tout, l'assurance vise à répartir les risques et à fixer le coût des primes en conséquence.

En s'opposant à la loi tant attendue sur la protection des renseignements génétiques confidentiels, c'est-à-dire le projet de loi S-201, Jacques Y. Boudreau, le président du Comité sur les tests génétiques de l'Institut canadien des actuaires a fait valoir qu'un élément essentiel d'une bonne assurance est un accès égal à l'information de la part des deux parties. Il y a clairement une tension entre notre droit de garder nos renseignements confidentiels et les intérêts commerciaux.

Nous passons beaucoup de temps à nous soucier de la façon dont un collecteur de données autorisé utilise nos données. Cependant, il y a eu plusieurs cas d'atteinte à la sécurité des données, que ce soit le piratage contre Sony, la fuite de courriels au parti démocrate ou le fiasco du site de rencontres Ashley Madison, qui prouvent que nos données personnelles peuvent se retrouver entre de mauvaises mains avec des conséquences dévastatrices. Parmi les personnes dont l'adresse courriel figurait sur la liste des clients d'Ashley Madison, certaines ont fait l'objet de chantage, d'autres ont subi des répercussions en milieu de travail, et trois personnes sont même allées jusqu'à se suicider. Sans parler du fait que certaines personnes se sont retrouvées sur la liste des utilisateurs sans même s'être inscrites, en raison de la conception laxiste du système.

Même si le Code criminel renferme des dispositions liées au piratage, notamment au méfait concernant les données et à l'utilisation non autorisée d'un ordinateur, elles ne traitent pas directement des répercussions du piratage sur la vie privée des gens. De toute évidence, de nombreux délinquants ne se font jamais prendre, mais certains se font pincer. Les entités qui gèrent les données devraient également en subir les conséquences lorsqu'elles n'ont pas pris les mesures nécessaires pour assurer la confidentialité.

Par conséquent, je suis en faveur d'une déclaration efficace des atteintes à la vie privée de la part des secteurs public et privé, et des mécanismes améliorés, y compris des pouvoirs d'ordonnance permettant au commissaire à la protection de la vie privée de préserver la confiance du public. J'appuie également un examen de nos lois en matière de protection des renseignements personnels tous les cinq ans.

Je vais terminer en vous faisant une révélation. Vous êtes en présence d'un cyborg, c'est-à-dire un être humain ayant subi une modification technologique. En fait, on m'a implanté une puce d'identification par radiofréquence dans la main à l'occasion de la dernière conférence de DEF CON. À l'heure actuelle, je n'ai qu'un seul super pouvoir: je peux ouvrir ma porte à l'université sans utiliser ma carte d'identité. Dans un avenir très rapproché, des dispositifs permettront aux gens d'avoir une vue ultra-précise, une ouïe très développée et des facultés mentales améliorées.

● (1125)

Les premières lois canadiennes sur la protection des renseignements personnels datent de l'époque où l'information était uniquement conservée sur papier, alors qu'aujourd'hui, grâce à l'infonuagique, nos données se retrouvent dans une multitude de serveurs situés un peu partout sur la planète. Notre prochain défi, qui nous tiendra occupés longtemps, sera de composer avec les répercussions de ces données qui font désormais partie intégrante de notre humanité.

Je vous remercie infiniment de votre attention. Je suis impatient de répondre à vos questions.

Le président: Merci beaucoup pour cet exposé très intéressant. Au risque de connaître la réponse, je ne vous demanderai pas où vous gardez vos clés de voiture.

Je vais maintenant céder la parole à M. Rubin.

Vous disposez de 10 minutes.

M. Ken Rubin (recherchiste d'enquête, protecteur des consommateurs, À titre personnel): La surveillance fait toujours peur.

Je suis de retour devant le Comité, étant donné l'intérêt que je porte à la protection de la vie privée et à la défense des droits depuis plus de 40 ans. J'ai commencé à travailler dans ce domaine au sein d'un groupe local de défense des libertés civiles qui s'intéressait à l'utilisation croissante des numéros d'assurance sociale comme moyen d'identification. À titre de recherchiste d'enquête, j'ai cherché de l'information sur les problèmes relatifs au couplage des données personnelles et, à cette époque, je témoignais au sujet des limites du projet de loi sur la protection des renseignements personnels du Canada et du partage des données secrètes.

Aujourd'hui, en cette ère numérique, les enjeux liés à la protection des renseignements personnels sont encore plus complexes et menaçants, étant donné les pratiques généralisées d'échange légal et illégal de renseignements personnels, l'extraction de mégadonnées et la surveillance de masse.

J'ai toujours cru que les Canadiens devaient avoir davantage accès aux renseignements les concernant et en rester maîtres et être mieux informés au sujet des intrusions. Le Canada ne peut pas continuer, trois décennies et demie plus tard, à avoir une loi sur la protection des renseignements personnels qui soit faible. Le fait qu'on se concentre davantage sur l'accès limité aux renseignements personnels plutôt qu'à la réglementation des intrusions incessantes de l'État et du secteur privé dans la vie privée des Canadiens fait en sorte qu'on se retrouve avec une protection insuffisante.

Il n'y a pas grand-chose dans la Loi sur la protection des renseignements personnels actuelle ni dans la LPRPDE qui peut mettre un terme à l'espionnage et à l'extraction de données en ligne et aux vérifications d'identité biométrique, limiter le recours croissant à des technologies de surveillance nouvelles et secrètes comme les dispositifs Stingray, qui permettent de mettre des téléphones cellulaires sur écoute, ou empêcher l'échange croissant de renseignements personnels sur les Canadiens avec des autorités étrangères.

Aucun ministre canadien n'est intervenu pour exiger une meilleure protection de la vie privée ou proposer des recours contre ce qu'Edward Snowden a mis au jour, à savoir les programmes ultrasecrets de surveillance de masse.

Aucun ministre canadien n'a mis en place des restrictions réglementaires concernant, par exemple, le traitement de la quantité croissante de renseignements personnels canadiens gardés ou transmis par les États-Unis en vertu de la Patriot Act ou ayant fait l'objet d'intrusions par d'autres entités étrangères.

Le récent document de travail du ministre de la Sécurité publique, Ralph Goodale, sur les pouvoirs de la police ne dissipe aucunement les préoccupations en matière de protection des renseignements personnels et des libertés civiles. Le président du Conseil du Trésor, Scott Brison, a déclaré, notamment devant le Comité, que plus et non moins de dossiers doivent être exemptés pour des raisons de sécurité nationale, ce qui ne vient pas non plus calmer les inquiétudes. M. Brison a indiqué que la commissaire à l'information ou, dans ce cas-ci, le commissaire à la protection de la vie privée aurait un droit d'examen et un accès limités à de tels dossiers de sécurité. Par conséquent, les débuts du gouvernement Trudeau sont loin d'être rassurants.

Nous devons renforcer la Loi sur la protection des renseignements personnels. Permettez-moi de vous parler brièvement des 10 secteurs dans lesquels on pourrait apporter des améliorations.

Ma première recommandation visant à améliorer la loi est conforme au témoignage de Lisa Austin recueilli précédemment. Nous devons commencer par encadrer les progrès limitant les violations de la vie privée, conformément à la Charte canadienne des droits et libertés. Cela dit, d'abord et avant tout, une nouvelle disposition de déclaration d'objet doit reconnaître la protection des renseignements personnels comme étant un droit protégé par la Constitution.

Ma deuxième recommandation consiste à réécrire la loi sur la protection des renseignements personnels et à créer un tout nouvel article qui fait ressortir les obligations évidentes et exécutoires ainsi que les restrictions sur le partage, le couplage, le profilage et le suivi des données.

Si une loi sur la protection des renseignements personnels doit devenir, comme ce devrait être le cas, une loi sur la protection des données plutôt qu'une loi désuète et limitée en matière de protection des renseignements personnels, il faudra y ajouter des dispositions plus claires et plus rigoureuses, de même que des restrictions concernant le partage des renseignements personnels.

Bien que le commissaire à la protection de la vie privée veule qu'il soit obligatoire de signaler rapidement au Commissariat les atteintes à la confidentialité des renseignements personnels dans le secteur public, il recommande que seulement certaines des personnes touchées soient informées, et il ne parle aucunement d'ordonnances exécutoires ou de pouvoirs du Commissariat d'imposer des pénalités en dépit du fait que de telles atteintes surviennent assez régulièrement. Je vais revenir là-dessus plus tard.

Ma troisième recommandation comporte trois volets. Tout d'abord, les gens devraient avoir le droit de consentir ou non à la collecte et à l'utilisation, par le gouvernement, de leurs renseignements personnels. Ensuite, il devrait y avoir moins d'exemptions, de fichiers inconsultables et de délais, de sorte que les gens puissent obtenir plus rapidement tous leurs renseignements. Enfin, tous les organismes, y compris le Cabinet du premier ministre, devraient être visés par la loi.

● (1130)

Quatrièmement, tout comme l'ancienne commissaire à la protection de la vie privée, Jennifer Stoddard, je recommande que l'information non enregistrée, comme les échantillons biologiques personnels, y compris l'ADN et les lectures d'iris, soit couverte. Les données volatiles, comme les puces d'identification par radiofréquence ou les renseignements recueillis par Singray, doivent être explicitement visées par les lois sur la protection des renseignements personnels au sein des secteurs publics et privés.

Cinquièmement, je recommande que le salaire et les avantages des fonctionnaires, de même que les violations commises par le secteur privé, ne soient plus considérés comme des renseignements personnels et qu'ils soient rendus publics. Par exemple, le montant exact des primes qui leur sont versées doit être divulgué. Le nom des entreprises, comme la banque qui s'est vu imposer une amende de 1,1 million de dollars par le CANAFE, et des personnes qui ont été reconnues coupables d'évasion fiscale doit également être révélé.

Ma sixième recommandation est la suivante: que le commissaire à la protection de la vie privée ait le pouvoir de rendre des ordonnances. Le commissaire Therrien approuve maintenant cette recommandation, mais des pouvoirs de contrainte et des sanctions plus sévères pour les violations de la vie privée seraient nécessaires pour limiter les atteintes à la vie privée et réglementer la circulation transfrontalière des renseignements. Son bureau aurait besoin de pouvoirs d'enquête étendus pour examiner les affaires concernant la circulation transfrontalière des renseignements et la collecte de mégadonnées. Ce n'est pas simplement une question de pouvoirs d'ordonnance.

Ma septième recommandation, conforme à celle du commissaire Therrien, consiste à ce qu'on élargisse l'éventail des motifs justifiant que lui et tous les Canadiens recourent aux tribunaux, y compris la collecte, l'utilisation et la communication abusive de renseignements personnels. À l'heure actuelle, les tribunaux ne peuvent être saisis que des affaires concernant l'accès à des dossiers personnels bloqués. Il aurait été utile aussi que le commissaire suggère qu'on donne aux personnes et aux groupes qui saisissent les tribunaux de tels cas d'atteinte à la vie privée les moyens de poursuivre le gouvernement. Il est important de noter que les personnes et les groupes peuvent toujours contester les ordonnances du commissaire, mais ils souhaitent que les tribunaux offrent une meilleure protection des renseignements personnels que ce n'est le cas actuellement avec le commissaire.

Ma huitième recommandation vise à séparer la surveillance lorsqu'il s'agit de l'accès à l'information et de la protection des renseignements personnels. En liant aussi étroitement les deux lois, on détruit la possibilité pour chacune d'aller plus loin dans la défense d'intérêts publics distincts et parfois contradictoires, ce qui consiste à veiller, dans le cas de l'une d'elles, à ce qu'il y ait des outils permettant la divulgation proactive et la transparence et des pratiques de responsabilisation et, dans le cas de l'autre, à limiter les intrusions dans la vie privée et à améliorer la souveraineté des données. Il est temps de dissocier la loi sur la protection des renseignements personnels de celle sur l'accès à l'information.

Comme neuvième recommandation, j'estime que pour avoir une loi sur la protection des renseignements plus efficace, le Comité doit étudier la possibilité d'apporter des changements radicaux à la Loi sur la protection des renseignements personnels tout en améliorant la Loi sur la protection des renseignements personnels et les documents électroniques, la LPRPDE. Les menaces couvertes par ces deux lois sont semblables et les recours qu'elle prévoit de même que leur but sont les mêmes: les Canadiens veulent un plus grand contrôle sur les renseignements personnels auxquels des tiers, de la police aux mercaticiens, ont accès.

Ma dixième et dernière recommandation vise à accroître la transparence — ce n'est pas étonnant —, de sorte que le public soit au courant de l'utilisation des pouvoirs relatifs aux atteintes à la vie privée. Les Canadiens sont peu conscients des systèmes et des moyens que les autorités utilisent pour mener des sondages qui peuvent les toucher. On sait peu de choses au sujet du coût de la surveillance et du budget que les services d'application de la loi et du renseignement de sécurité consacrent à cet égard. On ignore à quel moment et à quelle fréquence, par exemple, le dispositif Stingray est utilisé, de même que le coût qui s'y rattache. On ne sait pas exactement quelles sont les lois ni les autorités qui permettent une telle surveillance. Je peux penser à des dizaines de lois.

Le Comité, en plus de mener des examens périodiques de la loi sur la protection des renseignements personnels, devrait avoir un sous-comité chargé d'examiner et de remettre en question les lois qui permettent les atteintes et les intrusions dans la vie privée.

Permettez-moi de conclure en vous donnant un exemple qui démontre que le public est tenu dans l'ignorance en ce qui concerne la façon dont le système de surveillance canadien fonctionne. Récemment, j'ai découvert des données selon lesquelles le ministre de la Sécurité publique et ses collaborateurs avaient émis, entre 2014 et 2016, des permis à la GRC, au SCRS et au CSTC de la Défense nationale permettant à des entreprises privées anonymes d'avoir et de vendre du matériel de surveillance à des acheteurs non identifiés, possiblement un logiciel malveillant, un dispositif Stingray ou d'autres appareils de surveillance. Cela s'est fait sous le couvert d'un article du Code criminel du Canada.

● (1135)

Des documents indiquent, par exemple, que le SCRS a entretenu de longues relations avec certaines entreprises de surveillance et, dans un cas, un permis ministériel a été accordé de façon rétroactive. On ignore le type de surveillance qui a eu lieu, et il n'y a rien qui les oblige à en faire rapport, notamment en vertu de la loi sur l'écoute électronique.

L'idée est que, monsieur le président et mesdames et messieurs les membres du Comité, un ministre fédéral supervise cet accord de surveillance loin du regard du public. Sa préoccupation n'est pas de protéger la vie privée du public. C'est pourquoi d'autres personnes et moi avons présenté des recommandations pour que le Canada puisse renforcer sa législation inadéquate et remédier au laxisme de la réglementation en vue de protéger les citoyens.

Je vous remercie beaucoup.

Le président: Merci beaucoup, monsieur Rubin.

Nous allons maintenant passer à notre dernier témoin, M. Tamir Israel, de la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko.

Vous disposez de 10 minutes.

M. Tamir Israel (avocat, Samuelson-Glushko Clinique d'intérêt public et de politique d'Internet du Canada): Monsieur le président, et mesdames et messieurs les membres du Comité, bonjour. Je m'appelle Tamir Israel et je suis avocat à l'interne à la CIPPIC, soit la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko, au Centre de recherche en droit, technologie et société de l'Université d'Ottawa. La CIPPIC est une clinique d'intérêt public qui travaille à promouvoir les intérêts de la population dans des débats politiques à l'intersection où se rencontrent le droit et la technologie.

Tout d'abord, je tiens à vous remercier de nous avoir invités à témoigner devant vous aujourd'hui, de même que d'avoir entrepris cet important examen de la loi fédérale sur la protection des renseignements personnels, soit un élément central du cadre du Canada en matière de protection des renseignements personnels, de transparence et de responsabilisation.

Depuis l'adoption de la Loi sur la protection des renseignements personnels, à la fin des années 1970, le paysage politique entourant la protection des données a évolué considérablement, étant donné les changements fondamentaux dans les capacités techniques et les pratiques générales liées à la collecte et à l'utilisation des renseignements personnels. La loi fédérale sur la protection des renseignements personnels n'a tout simplement pas progressé au même rythme que ces changements importants, une réalité qui l'empêche de continuer à atteindre ses objectifs, compte tenu des capacités techniques et des incitatifs accrus pour recueillir et conserver les renseignements personnels à des niveaux sans précédent. La nature des objectifs des pratiques gouvernementales en matière de données a rapidement évolué au fil des années, depuis l'adoption de la Loi, dont le but initial était de réglementer les pratiques animées par des objectifs administratifs.

Aujourd'hui, les enjeux liés à la protection des renseignements personnels sont beaucoup plus diversifiés. Dans un contexte où les décisions s'appuient sur des données, communément appelées les « mégadonnées », de plus en plus d'organismes d'État sont amenés à ratisser large dans leurs efforts de collecte de données. De plus, la plupart du temps, la Loi s'applique pour examiner des activités motivées par des considérations liées à l'application de la loi et à la sécurité qui sont très éloignées des activités administratives qui ont mené à son adoption.

Enfin, le partage des données entre les organismes d'État nationaux et étrangers se déroule aujourd'hui d'une manière beaucoup plus informelle et intégrée sur le plan technologique que ce qu'on aurait pu prévoir à la fin des années 1970.

La Loi sur la protection des renseignements personnels a grandement besoin d'être modernisée et, à cet effet, la CIPPIC a examiné et appuie largement les recommandations formulées par le Commissariat à la protection de la vie du Canada au Comité concernant les modifications qui doivent être apportées pour s'assurer de relever les défis actuels en matière de protection des données. Nous reviendrons sur quelques-unes d'entre elles, ainsi que sur d'autres recommandations que nous avons élaborées dans notre mémoire. De plus, dans le mémoire que nous vous avons remis, nous avons fait quelques propositions relatives au libellé qui, espérons-le, orienteront votre examen de cette loi.

Le reste de nos recommandations vise à accroître la proportionnalité, la transparence et la reddition de comptes, et à corriger les lacunes découlant des développements technologiques.

Avant d'aborder ces grands thèmes, toutefois, notre première recommandation concerne la disposition de déclaration d'objet de la Loi sur la protection des renseignements personnels qui, selon nous, devrait être révisée afin de reconnaître explicitement les objectifs de la Loi: protéger les droits à la vie privée et accroître la transparence et la reddition de comptes de l'État en ce qui concerne l'utilisation des renseignements personnels. Le fait de reconnaître ces objectifs, comme on l'a fait à l'échelle provinciale, contribuera à aligner la loi sur ses objectifs quasi constitutionnels et à assurer l'efficacité de son application dans le cas où des ambiguïtés surviendraient à l'avenir, comme ce sera probablement le cas.

La nécessité et la proportionnalité sont des principes qui sont au coeur des régimes de protection des données dans le monde entier, mais qui sont absents de la Loi sur la protection des renseignements personnels désuète. Il est important de reconnaître explicitement ces principes dans la Loi et d'adopter d'autres mesures précises qui ne font pas partie de son mandat actuel, mais qui sont néanmoins essentielles pour veiller à ce que les données soient recueillies de façon proportionnelle.

Pour commencer, il faudrait mettre en oeuvre la recommandation du commissaire à la protection de la vie privée visant à reconnaître expressément la nécessité comme étant la norme régissant les pratiques de collecte de données. La nécessité est un principe de protection des données et fournit un contexte important pour évaluer si les données devraient ou non être recueillies, utilisées ou communiquées. La norme actuelle, qui exige seulement que les renseignements personnels en question doivent avoir un lien direct avec les programmes ou activités, est tout simplement trop vague en cette ère de mégadonnées, où les organisations sont de plus en plus encouragées à recueillir des données qui sont plus ou moins en lien avec leurs objectifs.

● (1140)

Deuxièmement, la Loi sur la protection des renseignements personnels n'impose aucune limite explicite quant à la conservation des données une fois qu'elles ont été recueillies de façon légitime. Le fait qu'il n'est pas obligatoire de fixer des limites raisonnables de conservation signifie que les données peuvent être conservées beaucoup plus longtemps que nécessaire, ce qui augmente de façon exponentielle le risque de violation des données et d'utilisation inappropriée. Cela peut même mener à la conservation indéfinie des données dont l'utilité est restreinte, ce qui mine énormément la proportionnalité d'une activité particulière.

Par exemple, notre clinique, de concert avec le Citizen Lab, à la Munk School of Global Affairs, a récemment publié un rapport sur l'utilisation d'un outil de surveillance appelé « simulateur de sites cellulaires ». Ces dispositifs imitent les tours de téléphonie cellulaire afin d'inciter tous les appareils mobiles à proximité à transmettre certains renseignements qui seront ensuite utilisés pour identifier ou suivre les individus ou les appareils. Ces dispositifs fonctionnent de façon brutale. Pour chaque cible contre qui ces dispositifs sont déployés, les données de centaines ou de milliers de personnes à proximité seront recueillies. Les données non ciblées recueillies sont utiles seulement immédiatement pour déterminer les ensembles de données qui appartiennent à la personne, la cible légitime de la recherche, et celles qui ne lui appartiennent pas, un objectif qui pourrait être atteint dans un délai de 24 à 48 heures suivant la collecte. Toutefois, comme la collecte de ces milliers d'ensembles de données non ciblées est légitime, ces ensembles de données pourraient être conservés indéfiniment. Ces grands ensembles de données peuvent alors être réutilisés à n'importe quel moment dans l'avenir et, sous réserve des régimes législatifs connexes tels que la Loi sur la communication d'information ayant trait à la sécurité du Canada, qui a été adoptée récemment dans le cadre du projet de loi C-51, ils peuvent être partagés à un large éventail d'organismes.

L'ajout d'une disposition qui établit clairement les limites de conservation chargerait non seulement les organismes d'État d'adopter des politiques de conservation claires, mais permettrait aussi au commissaire de remédier à une conservation déraisonnable selon des principes. Cela permettra de réduire le risque de violation des données et, de façon générale, d'augmenter la proportionnalité des pratiques de collecte de données.

Troisièmement, nous recommandons l'adoption d'une obligation de proportionnalité qui s'appliquerait à la collecte, à la conservation, à l'utilisation et à la divulgation des renseignements personnels par les organismes gouvernementaux en vertu de la Loi sur la protection des renseignements personnels. Ce serait comparable à son équivalent, que l'on trouve actuellement au paragraphe 5(3) de la LPRPDE. Comme vous l'ont dit d'autres témoins, la Loi sur la protection des renseignements personnels est un outil important pour veiller à ce que les principes de la Charte relatifs à la protection des droits fondamentaux à la vie privée soient pleinement respectés. Une obligation de proportionnalité ou de caractère raisonnable, calqué sur le paragraphe 5(3) de la LPRPDE, permettrait d'évaluer les considérations relatives à la Charte dans toutes les pratiques en matière de données. Elle donnerait également à la Loi sur la protection des renseignements personnels une certaine souplesse, lui permettant ainsi de suivre le rythme des changements technologiques en fournissant un principe général selon lequel on pourrait évaluer les développements futurs imprévus.

En plus de ces mesures de proportionnalité, on trouve des lacunes évidentes dans l'actuel cadre de transparence de la Loi sur la protection des renseignements personnels ainsi que des possibilités d'accroître la transparence des pratiques gouvernementales, ce qui pourrait favoriser la reddition de comptes et la confiance du public.

Nous encourageons d'emblée l'adoption de la recommandation du commissaire à la protection de la vie privée concernant la dérogation aux obligations en matière de confidentialité prévues dans la Loi. Cela permettrait que des renseignements importants d'intérêt public soient divulgués en temps opportun.

Ensuite, la Loi sur la protection des renseignements personnels devrait être modifiée, de façon à ce que les divers pouvoirs de surveillance électronique prévus dans le Code criminel soient assortis d'obligations de déclaration statistique. Comme M. Rubin l'a mentionné, les obligations de déclaration statistique étaient ce qui caractérisait les régimes de surveillance électronique et se rattachent à certaines activités de surveillance électronique, telles que l'écoute électronique, mais ces activités ont, en grande partie, été remplacées par d'autres activités de surveillance électronique qui ne sont pas assujetties à de telles obligations.

Une enquête menée par le commissaire à la protection de la vie privée a récemment révélé que les organismes d'application de la loi eux-mêmes n'avaient pas une idée claire de la portée de leurs propres pratiques en ce qui concerne la collecte de renseignements sur les abonnés de la part des entreprises de télécommunications. Il est essentiel de comprendre la nature et la portée des pratiques de surveillance de l'État, compte tenu de l'évolution rapide des pratiques dans ce domaine. Par conséquent, l'inclusion dans la Loi sur la protection des renseignements personnels d'une obligation de déclaration statistique qui s'appliquerait à tout le spectre des pouvoirs de surveillance électronique fournirait un important mécanisme de transparence.

Enfin, l'adoption d'une obligation générale en vertu de laquelle les organismes d'État seraient tenus d'expliquer leurs pratiques permettrait d'accroître considérablement la transparence. Bien que la Loi oblige actuellement les organismes gouvernementaux à expliquer aux personnes concernées les fins pour lesquelles leurs renseignements personnels sont recueillis et utilisés, il manque une obligation générale au sujet des pratiques.

Une obligation inspirée du principe de transparence de la LPRPDE serait bénéfique. Si ce principe est adopté, il devrait remédier aux problèmes découlant de la non-transparence algorithmique, ce qui entraînerait une obligation d'expliquer la logique de tout mécanisme de prise de décisions automatisé adopté par l'État.

Nous avons quelques suggestions à propos de mesures de reddition de comptes et de conformité que je vais vous soumettre par écrit et que vous pourrez examiner ultérieurement.

Je voulais revenir très rapidement sur les quelques recommandations concernant les développements technologiques qui ont fait en sorte que la Loi sur la protection des renseignements personnels est devenue lacunaire.

● (1145)

Nous recommanderions de modifier la définition de « renseignements personnels » afin qu'elle corresponde davantage à celle figurant dans la LPRPDE. La définition actuelle s'applique uniquement aux renseignements personnels qui sont consignés, alors que de nombreuses pratiques modernes de collecte et d'utilisation de données ne consignent jamais systématiquement les données personnelles, mais ont tout de même une incidence importante sur la vie privée des gens.

De plus, nous appuierions la recommandation du commissaire à la protection de la vie privée du Canada visant à adopter l'obligation explicite de mettre en place des mesures de protection technologiques ainsi que des obligations à l'égard du signalement d'atteintes à la vie privée.

Enfin, et très brièvement, nous appuierions également la recommandation du commissaire à la protection de la vie privée d'officialiser l'exigence concernant l'évaluation des facteurs relatifs à la vie privée, et nous recommanderions un moyen de faciliter la participation du public dans le processus, de façon à ce que les discussions sur les programmes qui portent atteinte à la vie privée se déroulent aux étapes préliminaires.

Merci. C'est ce qui met fin à mon exposé.

● (1150)

Le président: Merci beaucoup, monsieur Israel, et merci à tous nos témoins.

Nous allons maintenant passer à la période de questions. Je demanderais aux membres du Comité et aux témoins d'être aussi concis que possible.

Pour le premier tour de sept minutes, c'est M. Long, du Parti libéral, qui va ouvrir le bal.

M. Wayne Long (Saint John—Rothesay, Lib.): Bienvenue à tous. Je suis heureux de revoir tout le monde. C'est un plaisir de vous avoir de nouveau parmi nous, monsieur Rubin.

Comment va l'exploitation?

M. Ken Rubin: Les récoltes arrivent, ce qui n'est pas le cas des libéraux.

M. Wayne Long: Monsieur Rubin, permettez-moi d'être honnête, lors de votre dernière comparution, vous prôniez l'accessibilité par défaut des renseignements. Vous êtes ici aujourd'hui pour défendre la protection des renseignements personnels et la vie privée des gens. Comment arrivez-vous à défendre les deux?

M. Ken Rubin: D'une part, il y a certaines choses que l'État n'a pas besoin de savoir, ou s'il doit le savoir, certaines restrictions ou règles doivent s'appliquer. C'est très différent des enjeux d'intérêt public, où le public doit connaître l'information. Il doit y avoir une reddition de comptes.

D'autre part, j'aimerais établir un parallèle avec les accords de divulgation proactive et ainsi de suite. Du côté de la Loi sur la protection des renseignements personnels, l'article 48 porte sur la collecte de l'information. Par conséquent, dans les années 1980, il y avait des milliers d'accords de partage de données personnelles entre les différents ministères, les provinces, à l'échelle internationale, mais du côté de l'accès à l'information, il n'y avait presque rien. Il n'est aucunement question de transparence. Il y a donc une dichotomie ici.

Je n'irai pas plus loin, si ce n'est pour dire qu'à mon avis, les deux sont compatibles à certains égards, mais si on veut maximiser leur efficacité, il vaut mieux les dissocier.

M. Wayne Long: D'accord, merci.

Vous avez été cité dans un article — un article paru dans le *Kamloops This Week* au sujet du district scolaire de Gold Trail, dans lequel un conseiller a été censuré.

M. Ken Rubin: Oui.

M. Wayne Long: Un rapport a été publié; les gens voulaient de l'information et, évidemment, le conseil scolaire a bloqué une grande partie de l'information. Je vous cite:

> Il y a des documents qui ne sont pas communiqués, comme dans ce cas-ci, relativement à des questions disciplinaires, mais pour la crédibilité des parties, en vertu de l'obligation de rendre compte, on pourrait au moins espérer un résumé du dossier.

Dans ce cas-ci, protégeriez-vous les droits de la personne ou le droit du public de connaître l'information? Encore une fois, comment arrivez-vous à concilier les deux?

M. Ken Rubin: C'est difficile. Je ne dis pas que tous les détails doivent être divulgués. Il y a des questions d'ordre personnel qui peuvent être délicates, mais lorsqu'on est un conseiller au sein d'un conseil scolaire public, le public ou les autres conseillers ont le droit de savoir. Ce journaliste de la Colombie-Britannique ignorait toute l'affaire. Pour la crédibilité de tout le monde, il faut qu'il y ait un niveau minimal de transparence, tout en protégeant la vie privée de la personne jusqu'à un certain point.

M. Wayne Long: Vous voyez le...

M. Ken Rubin: Oui, d'accord.

M. Wayne Long: Où trouvez-vous cet équilibre?

M. Ken Rubin: Vous venez tout juste de donner un exemple, et j'essaie d'expliquer comment je traiterais cet exemple. Les gens ont différentes perceptions de ce qui est privé et de ce qui ne devrait pas l'être. Toutefois, beaucoup de gens ont des idées fausses sur ce qui devrait être public et estiment que la surveillance des gens devrait toujours demeurer un secret d'État. Voilà le problème. On cache trop de choses. Et ce n'est pas parce qu'on a une meilleure compréhension de la protection de la vie privée.

● (1155)

M. Wayne Long: Merci.

Monsieur Keenan, je vous remercie de votre exposé.

Voici maintenant une citation tirée de l'un de vos articles. Vous avez dit: « Nous sommes déjà dans une société de surveillance, et il n'y aura pas de retour en arrière. »

M. Thomas Keenan: C'est vrai.

M. Wayne Long: Dans cet article, vous dites également que vous comptez toujours les caméras de surveillance partout où vous allez.

Combien en avez-vous compté aujourd'hui?

M. Thomas Keenan: J'en ai compté 14 seulement en venant ici.

J'ai rencontré ma femme en comptant les caméras de surveillance à San Francisco, et il nous a fallu une heure pour en trouver 100. Nous sommes ensuite allés à notre premier rendez-vous. Je peux vous dire que c'était un rendez-vous merveilleux.

Des voix: Oh, oh!

M. Wayne Long: Vous les avez donc comptées aujourd'hui.

M. Thomas Keenan: En fait, aujourd'hui, je n'ai pas vraiment eu besoin de les compter, parce que chacun d'entre vous a un téléphone cellulaire dans sa poche. Il y a des caméras qui sont si petites qu'on ne pourrait pas le savoir... Je regarde autour de moi, et j'essaie de voir s'il serait facile pour quelqu'un d'y cacher une caméra.

On voit toujours cela à DEF CON. Les gens installent des dispositifs clandestins, pas seulement des caméras, mais des appareils qui utilisent votre Wi-Fi. Ils les laissent au Starbucks et ils peuvent rester là pendant des mois à transmettre toutes les données.

Donc oui, nous sommes dans une société de surveillance.

M. Wayne Long: Je vous cite de nouveau: « Ces caméras sont installées pour deux grandes raisons ». Vous venez de Calgary et, dans cette ville, on dit qu'il y a plus de 3 500 caméras. Il est ensuite question d'Edmonton, où il y en a plus de 3 000. On en retrouve dans tous les autobus.

Ces gens disent que ces caméras sont installées pour la protection des biens, la sécurité publique, etc.

Êtes-vous d'accord?

M. Thomas Keenan: Tout à fait.

M. Wayne Long: D'accord.

M. Thomas Keenan: Absolument.

Par exemple, prenez l'attentat à la bombe au marathon de Boston. Les meilleures images ont été filmées à partir d'une caméra de surveillance d'un magasin sur l'avenue Massachusetts, et la police était très heureuse qu'elle se trouve à cet endroit. Prenez les émeutes de la Coupe Stanley à Vancouver. Il y avait des vidéos prises par les citoyens. Cela a donc soulevé une question importante au sujet de la protection de la vie privée, sur laquelle le commissaire provincial a dû se prononcer. La police pourrait-elle comparer la base de données sur les permis aux photos des gens en train de piller des magasins afin de les identifier?

Elle a pris une décision très sage. Elle a proposé de soumettre la vidéo des scènes de pillage à une tierce partie, soit les responsables de la délivrance des permis en Colombie-Britannique, afin qu'elle puisse l'examiner, mais il fallait avoir un juge pour desceller les données.

Je crois qu'il faut davantage de surveillance; autrement, on se livre à une expédition de pêche. Dans mon livre, je donne l'exemple d'un homme qui garait sa voiture dans l'espace de stationnement numéro 11 et qui a été identifié par la police comme étant un membre de l'entourage d'un mafioso, et cela, uniquement parce que l'homme qui se stationnait à côté de lui, dans l'espace numéro 12, était un chef de la mafia. Étant donné qu'ils se saluaient tous les matins, l'homme a été considéré comme une « relation connue ».

M. Wayne Long: Vous avez également parlé des panneaux d'avertissement nous informant de la présence de caméras.

Croyez-vous que des panneaux d'avertissement devraient être installés?

M. Thomas Keenan: En fait, sur le site Web du CPVP, on recommande d'installer des panneaux d'avertissement et d'y indiquer pour quelle raison et en vertu de quelle loi des caméras sont utilisées, de même que les personnes à qui s'adresser.

Devinez quoi? Toronto donne le numéro de téléphone de la police. À Calgary, on dit qu'il faut composer le 311. On peut attendre jusqu'à deux heures lorsqu'on appelle à ce numéro, alors ce n'est pas très efficace, d'autant plus que seules les gares du train léger ont des panneaux. Lorsqu'on va ailleurs, on ne trouve aucun panneau d'avertissement.

M. Wayne Long: Encore une fois, dans cet article du *Calgary Herald*, on dit que les caméras ne dissuadent pas les gens de commettre des crimes.

M. Thomas Keenan: Selon une étude menée au Royaume-Uni, il s'agirait d'un crime par 10 000 caméras...

Elles peuvent dissuader les gens. Évidemment, si les gens savent qu'ils sont surveillés, il se peut qu'ils modifient leur comportement, mais les bonnes vieilles méthodes policières permettent de résoudre la plupart des crimes.

M. Wayne Long: Croyez-vous que s'il y avait plus de panneaux d'avertissement, il y aurait moins de crimes?

M. Thomas Keenan: Non, je crois simplement que les gens...

Le président: Monsieur Long, vos sept minutes sont écoulées depuis longtemps. Vous avez posé de bonnes questions. Si nous avons le temps, nous y reviendrons.

Monsieur Jeneroux, vous disposez de sept minutes.

M. Matt Jeneroux (Edmonton Riverbend, PCC): M. Long a l'air tellement déçu.

Le président: Moi aussi, en quelque sorte. J'aurais préféré ne pas l'interrompre, mais...

M. Matt Jeneroux: Merci à vous tous d'être ici aujourd'hui. Je pense que pour certains d'entre vous, ce n'est pas la première fois que vous témoignez. Monsieur Keenan, il s'agit de votre première comparution devant le Comité. Encore une fois, je vous remercie de votre présence.

J'aimerais parler brièvement de l'évolution rapide de la technologie. Nous avons une loi qui est en vigueur depuis 1983. Toutefois, il y a un certain nombre de politiques qui ont été mises en oeuvre à l'échelle du gouvernement pour composer avec la nouvelle technologie.

Si nous disons: voici ce que nous voulons faire en 2016, tel qu'indiqué dans le rapport du commissaire à la protection de la vie privée, comment peut-on s'assurer que notre mesure législative ne sera pas tout de suite désuète, étant donné l'évolution de la technologie?

Pourriez-vous nous dire comment vous envisagez cela et aussi répondre à l'argument des politiques par opposition à la loi? Si cela ne vous dérange pas, j'aimerais tous vous entendre là-dessus.

● (1200)

Le président: Allez-y, monsieur Israel.

M. Tamir Israel: Merci.

J'aimerais souligner que la LPRPDE, le pendant de la Loi sur la protection des renseignements personnels, adoptée plus récemment, comprend un cadre fondé sur des principes plutôt qu'un cadre plus normatif. Certaines de nos recommandations, ainsi que des recommandations d'autres témoins, tendent à proposer l'adoption d'un cadre fondé sur des principes. Je crois qu'un tel cadre permet à la loi de mieux évoluer. De nos jours, les lois doivent être modifiées à l'occasion en fonction des changements technologiques. Donc, l'ajout d'un examen quinquennal est une bonne idée. Je crois que l'ajout de principes, comme une obligation générale de proportionnalité, permet à la loi d'évoluer en fonction des changements technologiques que nous ne pouvons pas prévoir, sauf M. Keenan qui a une fenêtre sur l'avenir.

M. Matt Jeneroux: Madame McPhail, auriez-vous quelque chose à ajouter?

Mme Brenda McPhail: Je suis d'accord avec Tamir. Nous devons nous assurer que la loi est fondée sur des principes plutôt que sur des détails et des points précis. L'adoption d'un critère de nécessité aussi serait utile, car peu importe la technologie utilisée pour recueillir les renseignements, il est toujours utile de se demander si l'on a besoin des renseignements en question. Ont-ils été recueillis de façon appropriée et correctement? La définition de « façon appropriée » et « correctement » pourrait changer en fonction des changements technologiques, mais l'idée de s'assurer que les choses sont faites selon des principes de base ne change pas; cela nous permet une plus grande souplesse et assure la pertinence de la loi au fil des changements.

M. Matt Jeneroux: Quelqu'un d'autre voudrait intervenir?

Monsieur Rubin, allez-y.

M. Ken Rubin: J'aimerais simplement souligner une chose. En réalité, la Loi sur la protection des renseignements personnels au Canada existe depuis la fin des années 1970, car j'exerçais mes activités en vertu de la Partie IV de la Loi canadienne sur les droits de la personne. C'est donc une loi intéressante.

C'est ce que tente de faire le Commissaire à la protection des renseignements personnels, dans une certaine mesure, mais j'ajouterais simplement qu'à mon avis, il serait utile de disposer d'un bureau de la technologie — ce que le Conseil des sciences du Canada a déjà proposé — qui aurait pour mandat d'évaluer les conséquences de la technologie de plusieurs points de vue, notamment celui de la protection des renseignements personnels. Nous aurions ainsi un organisme responsable d'examiner et de proposer constamment de nouvelles idées concernant la technologie et ses incidences. Il semble y avoir un manque de continuité; il y a toujours quelque chose.

C'est tout ce que j'ajouterais, outre que les choses ont effectivement beaucoup changé depuis la première partie. Mais, avec le NAS et les métadonnées, notamment, les options possibles demeurent similaires.

Le président: Monsieur Keenan, allez-y.

M. Thomas Keenan: Je suis professeur. Vous ne serez donc pas surpris si je dis qu'il faut financer plus de recherches. C'est ce que fait déjà le Commissaire à la protection des renseignements personnels, mais il pourrait en faire davantage à cet égard. J'aimerais vous parler d'un autre concept.

À une époque, j'ai pris un congé sabbatique pour travailler chez Northern Telecom. Mon mandat était de trouver de nouvelles fonctions à ajouter à leurs téléphones. J'ai trouvé une solution au problème des télécommerçants. Ces gens m'interrompaient sans cesse pendant le souper. Je me suis dit que je devrais pouvoir attribuer une valeur pécuniaire à l'utilisation de mon téléphone. Si je m'ennuie, la valeur pourrait être de 0 $ ou de 0,10 $. Si je suis en train partager un repas romantique extraordinaire et que vous m'interrompez, il vous en coûtera 1 500 $. Si vous êtes d'accord, je vous facture pour la conversation. Nortel n'a pas ajouté cette fonction à ces téléphones, mais moi, j'ai adopté l'idée. Lorsque quelqu'un m'appelle, je lui dis: « Cet appel vous coûtera 100 $/l'heure; j'accepte Visa ou MasterCard. »

Quel est le lien avec la discussion d'aujourd'hui? Les gens doivent accorder de l'importance à leur vie privée. Si vous utilisez Google, Gmail et YouTube, entre autres, vous valez environ 800 $ par année pour Google. Il n'y a aucun moyen de payer Google; ces services sont offerts gratuitement. Par contre, l'entreprise vend vos renseignements personnels. C'est ce que l'on appelle le concept de la surveillance capitaliste. C'est ce dont parle Shoshana Zuboff, professeure à Harvard. Il y a un aspect économique à tout cela. Peut-être devrions-nous dire aux gens que s'ils estiment que leur vie privée a une valeur, ils devraient pouvoir se faire payer, comme dans le cas des télécommerçants. Si vous voulez donner vos renseignements personnels à une société d'assurance parce que vous voulez le rabais qu'elle vous offre, d'accord, mais vous le faites en toute connaissance de cause. La loi doit expliquer clairement, dans une certaine mesure, ce que les sociétés peuvent faire avec vos renseignements.

M. Matt Jeneroux: Merci.

J'ignore si tout a été répondu, mais j'imagine que nous aurons l'occasion d'y revenir avec d'autres témoins.

Brièvement, madame McPhail, j'aimerais obtenir votre opinion sur l'élargissement de l'application de la loi. Une des recommandations est d'élargir l'application de la loi au Cabinet du premier ministre et aux cabinets des ministres. Cette recommandation ne faisait pas partie de celles formulées par le Commissaire à la protection des renseignements personnels il y a quelques années. Qu'en pensez-vous?

● (1205)

Mme Brenda McPhail: Brièvement, c'est une chose que j'appuierais. Les Canadiens ont le droit de savoir que, peu importe l'ordre de gouvernement ou le niveau de pouvoir, leurs renseignements personnels sont recueillis et conservés de manière sécuritaire et qu'ils ont le droit concurrent de présenter des demandes d'information en vertu d'autres lois. Je crois qu'il serait sage et logique que la loi s'applique également aux échelons supérieurs du gouvernement.

M. Matt Jeneroux: Bien.

Le président: Monsieur Blaikie, vous avez la parole pour sept minutes.

M. Daniel Blaikie (Elmwood—Transcona, NPD): Merci aux témoins pour ces exposés.

Je comprends qu'un cadre davantage fondé sur des principes permettrait à la loi actuelle d'évoluer au rythme des changements technologiques.

Concernant l'application de la loi ou l'idée de nous assurer que les gens comprennent mieux leurs droits et comment les protéger, pourriez-vous nous donner des détails sur la forme que cela pourrait prendre pour éviter que l'avis émis aux utilisateurs des services gouvernementaux, par exemple, qui acceptent que leurs renseignements personnels soient utilisés à d'autres fins ne soit pas dissimulé dans les petits caractères? Auriez-vous des exemples concrets de la forme que cela pourrait prendre? Quelle serait la différence par rapport à la situation actuelle?

M. Thomas Keenan: Si vous lisez les nouveaux règlements adoptés par l'Union européenne concernant la protection générale des données, vous constaterez que les amendes pour les contrevenants sont extrêmement salées; on parle d'environ 4 % du chiffre d'affaires annuel d'une société. Les gens ont peur. Cela fait même réfléchir les gens de Calgary, car ils font des affaires en Europe. Des gens m'ont dit qu'il faut faire attention, car les amendes peuvent être très élevées si l'on atteint à la vie privée des particuliers. Peut-être que de telles amendes feraient réfléchir.

M. Daniel Blaikie: Je suis désolé, car les détails de l'affaire ne me sont pas familiers et j'ignore si vous pourrez me répondre, mais j'ai entendu dire qu'une action en justice avait été intentée en Britannique contre Facebook pour utilisation de renseignements personnels. Un des problèmes, c'est que l'entente d'utilisation de Facebook qu'acceptent les utilisateurs comprend une clause qui stipule qu'aucune action en justice ne peut être intentée contre l'entreprise ailleurs qu'en Californie. Sans préjuger du résultat de l'affaire, même si les Canadiens sont protégés par certaines des meilleures lois en matière de protection des renseignements personnels, à quel point sommes-nous vulnérables? Que peut-on faire concernant les ententes que les gens acceptent sans vraiment les lire et qui les obligent à intenter des actions en justice hors de leur territoire où ils seraient protégés par une loi renforcée?

M. Tamir Israel: Sans préjuger du résultat de l'affaire, la question est de savoir si, par l'entremise de diverses clauses contractuelles, une entreprise comme Facebook qui a des millions d'abonnés au Canada peut se soustraire aux lois canadiennes. Si la décision confirme qu'une telle entreprise peut se soustraire à nos lois, nous devrons demander une nouvelle réforme législative pour empêcher expressément l'application de telles clauses. Il n'est pas nécessaire de tout interdire. La Loi sur la protection des renseignements personnels est un peu protégée contre ce genre d'activités en raison de la façon dont elle s'applique aux entreprises privées.

Il sera très important à l'avenir de nous assurer que, dans certains cas, les normes et lois canadiennes s'appliquent aux entités internationales exploitées à l'étranger afin d'assurer un certain niveau de transparence et la protection des renseignements personnels conformément aux normes canadiennes.

M. Daniel Blaikie: Une des recommandations faites au comité est que le gouvernement devrait consulter le CPVP avant de déposer un projet de loi pour vérifier quelles seraient les conséquences sur la protection des renseignements personnels. Nous savons que les accords commerciaux internationaux et autres types d'accords avec des gouvernements ont une incidence sur la protection des renseignements personnels. Selon vous, en plus des projets de loi, cela devrait-il s'appliquer à tout accord légal important conclu par le gouvernement?

M. Tamir Israel: Je crois que oui. Par exemple, en Colombie-Britannique, un comité menant un examen du pendant provincial de la Loi sur la protection des renseignements personnels ignorait qu'un accord commercial avait été conclu, même si certains départements au sein du gouvernement provincial avaient participé aux négociations de l'accord en question. De nos jours, ces accords sont si multilatéraux et ont un impact sur tellement d'aspects de la vie de tous les jours qu'il est nécessaire d'adopter un processus de consultation plus intégré; ils ignoraient qu'un mécanisme adopté pourrait avoir un impact sur leur loi. Nous pourrions dire la même chose concernant d'autres aspects de la Loi sur la protection des renseignements personnels et de la LPRPDE. Il sera très important de trouver une façon d'incorporer ce genre de consultation dès le début, puisque de plus en plus de décisions seront prises dans ce genre de contexte.

J'ignore si Mme McPhail voudrait intervenir, mais l'ACLC a publié un rapport plus tôt aujourd'hui sur la façon de mieux tenir compte des protections constitutionnelles dans les processus législatifs. Vous voudrez peut-être l'interroger sur le sujet.

● (1210)

M. Daniel Blaikie: D'accord. Je sais que M. Rubin voudrait intervenir.

M. Ken Rubin: Une méthode d'application pourrait être de pénaliser les gens.

Ce qui me préoccupe par rapport à la loi dans sa forme actuelle, c'est que les articles relatifs à l'utilisation, à la rétention et à la collecte de données sont très vagues. C'est la raison pour laquelle je dis qu'il faut renforcer la loi. On ne peut être précis à tous les égards, mais le cheminement transfrontalier de données? Allons. Ça ne date pas d'hier. Si nous pouvons constater ce cheminement, nous pouvons, dans une certaine mesure, l'anticiper. Sans langage précis à ce sujet, nous n'avons rien à appliquer. Nous avons besoin de langage précis, notamment en ce qui concerne les métadonnées et les données biométriques. Sans contenu, nous n'avons rien à appliquer.

M. Daniel Blaikie: Madame McPhail, auriez-vous quelque chose à ajouter?

Le président: Nous ne vous entendons pas, madame McPhail.

Mme Brenda McPhail: Les difficultés technologiques sont à propos dans le cadre de la discussion d'aujourd'hui.

M. Israel faisait référence au rapport *Charter First* que nous venons tout juste de publier. Il s'agit d'un exposé de position de l'ACLC dans lequel nous faisons valoir que tous les projets de loi proposés au Canada devraient d'abord faire l'objet d'un examen fondé sur la Charte. Cela est conforme avec la recommandation selon laquelle toute loi ayant des conséquences sur la vie privée des gens devrait faire l'objet d'un examen de la part d'un organisme compétent. Dans le cas de la Loi sur la protection des renseignements personnels, ce serait, à mon avis, le Commissaire à la protection des renseignements personnels. De façon générale, nous appuyons l'adoption de protections multiples faisant en sorte que les droits protégés par la Charte — et la vie privée est un droit quasi constitutionnel — font toujours l'objet d'un examen et d'une étude, peu importe l'activité relative. Qu'il s'agisse d'un traité multilatéral, d'un accord commercial, d'un projet de loi ou d'un nouveau système de traitement des données, tous devraient faire l'objet d'une étude par une entité compétente afin d'évaluer, notamment, les risques relatifs à la protection des renseignements personnels.

Le président: Monsieur Lightbound, vous avez la parole pour sept minutes.

M. Joël Lightbound (Louis-Hébert, Lib.): Je tiens d'abord à préciser que s'il me reste du temps, je laisserai la parole à M. Erskine-Smith.

Merci à tous d'avoir accepté notre invitation. Ma première question s'adresse à Mme McPhail et à M. Israel.

De façon générale, la Loi sur la protection des renseignements personnels interdit le partage de renseignements personnels. Toutefois, on retrouve, au paragraphe 8(2), une grande liste d'exceptions, comme le partage de renseignements personnels effectué conformément à une loi ou à un règlement fédéraux. Puis, il y a eu l'adoption du projet de loi C-51 qui permet le partage de renseignements entre 17 institutions ou organismes gouvernementaux, si je ne m'abuse.

Quelle approche devrait-on adopter par rapport au partage de renseignements? Auriez-vous des recommandations à nous faire à cet égard?

M. Tamir Israel: Une de nos recommandations est qu'il faudrait adopter un mécanisme général de proportionnalité. Tout comme son pendant du secteur privé, la LPRPDE, selon nous, un tel mécanisme permettrait un contrôle de ces exceptions. Cela ne signifie pas que toute exception pourrait être systématiquement outrepassée, mais le principe de proportionnalité pourrait être ajouté à l'application de ces exceptions, si vous voyez ce que je veux dire. C'est ce que nous proposons par rapport aux exceptions.

La liste actuelle des exceptions est très longue. Les tribunaux ont aussi défini et limité certaines exceptions en fonction de l'interprétation de la Charte, entre autres. Nous n'avons aucune recommandation sur la façon d'aborder des exceptions précises, mais, selon nous, l'adoption d'une obligation générale de proportionnalité permettrait de limiter davantage l'application problématique de ces exceptions.

● (1215)

Mme Brenda McPhail: Nous appuyons la proposition relative à la proportionnalité. Si le comité décide d'entreprendre une étude détaillée de toutes les exceptions, nous tenons à préciser que de façon générale, selon nous, le nombre d'exceptions devrait être limité et celles-ci devraient être aussi restreintes que possible, et ce, dans tous les cas.

M. Joël Lightbound: Si vous pouviez nous faire parvenir vos recommandations écrites par rapport aux exceptions et à la façon d'en réduire le nombre, nous vous en serions très reconnaissants.

Ma deuxième question concerne les métadonnées. Il en a été brièvement question. Aucune loi canadienne ne définit ce que sont les métadonnées. Il y a quelques années, Joyce Murray a déposé un projet de loi d'initiative parlementaire pour définir ce que sont les métadonnées, mais elle proposait d'ajouter cette définition à la Loi sur la défense nationale. Selon vous, serait-il pertinent d'ajouter une définition des métadonnées à la Loi sur la protection des renseignements personnels pour régler la question?

Encore une fois, ma question s'adresse à M. Israel et à Mme McPhail.

M. Tamir Israel: Pour l'adoption, il serait utile de préciser que les métadonnées ne sont pas englobées dans la définition de « renseignements personnels », dans la Loi, où il se trouve des ambiguïtés. L'adresse IP (de protocole Internet) est un bon exemple. On entend souvent que, parce que sa connexion à un nom exige trois ou quatre étapes, elle ne constitue pas un renseignement personnel. C'est parce que la définition de « renseignement personnel » est liée à des renseignements qui se rapportent à quelqu'un d'identifiable. On peut en laisser une partie à l'interprétation du commissaire à la protection de la vie privée, etc. En Europe, je pense qu'on a publié des directives sur des difficultés précises que présentent les métadonnées comme les adresses IP, dans le sens où il faut les considérer comme des renseignements personnels.

Je pense qu'une partie du problème de l'inclusion des métadonnées dans une définition juridique réside dans l'évolution constante de la notion. Peut-être qu'un renvoi à un règlement, qui permettrait l'adoption d'une définition évolutive, serait le meilleur moyen de résoudre ce problème particulier et de s'assurer que ce type de données reste protégé par la Loi sur la protection des renseignements personnels.

Mme Brenda McPhail: Je pense que nous serions un peu plus directs que M. Israel, en disant simplement que, pour nous, les métadonnées doivent être une catégorie protégée. La jurisprudence selon laquelle les métadonnées peuvent révéler beaucoup de détails personnels intimes des renseignements biographiques d'ordre personnel est maintenant assez abondante.

Quant au mécanisme à employer, peut-être que la réglementation donne d'excellents résultats dans les détails, mais nous privilégions une déclaration générale sur les types de renseignements protégés, qui figurerait directement dans la loi.

M. Joël Lightbound: Monsieur Erskine-Smith, je vous cède mes deux dernières minutes.

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

Ma première question concerne le modèle de dommages-intérêts de la Loi sur la protection des renseignements personnels et les documents électroniques. Proposeriez-vous le même, qu'il s'agisse de dommages-intérêts accordés par un tribunal administratif ou par la Cour fédérale, pour la Loi sur la protection des renseignements personnels? Vous pouvez tous répondre.

M. Tamir Israel: La question est complexe, mais, de prime abord nous le ferions et nous irions probablement plus loin que l'actuelle Loi sur la protection des renseignements personnels et les documents électroniques. Essentiellement, le mécanisme qu'elle prévoit s'apparente plus à une amende. La mise en oeuvre est difficile, parce qu'il faut satisfaire à des normes de preuve très rigoureuses avant de pouvoir démontrer le viol délibéré de la vie privée, tandis qu'un régime de sanctions pécuniaires administratives serait plus adapté à ces types de régimes réglementaires.

Dans notre exposé, nous avons précisément laissé entendre, mais très rapidement, la possibilité d'envisager un droit privé d'action. Il surgit un problème, bien sûr, quand on expose l'État à des amendes et, manifestement, ça doit...

M. Nathaniel Erskine-Smith: Le droit privé d'action existe cependant dans la Loi sur la protection des renseignements personnels et les documents électroniques, sous le régime des articles 14 à 17.

M. Tamir Israel: Effectivement.

M. Nathaniel Erskine-Smith: Nous envisageons donc ce genre de modèle.

M. Tamir Israel: Ce mécanisme est lié au recouvrement des dommages-intérêts. Je le modifierais légèrement, parce que celui de la Loi sur la protection des renseignements personnels et les documents électroniques dépend d'une plainte. Il faut porter plainte, passer par tout le processus et, essentiellement, recommencer à la Cour fédérale dans l'espoir d'obtenir des dommages-intérêts. Très peu sont prêts à s'aventurer dans ce processus.

● (1220)

M. Nathaniel Erskine-Smith: Une sanction administrative suivie d'une forme d'examen judiciaire à la Cour fédérale.

M. Tamir Israel: Et, peut-être, un droit privé, indépendant, d'action, parallèlement, qu'il vaudrait la peine d'envisager.

M. Nathaniel Erskine-Smith: Quelqu'un n'est pas d'accord?

M. Thomas Keenan: Je voudrais seulement ajouter un détail. Je faisais partie d'une commission qui a dépensé 2 millions de dollars de sanctions administratives empochés par la Commission des valeurs mobilières de l'Alberta. Nous les avons employés à sensibiliser le public aux investisseurs. D'après moi la sensibilisation serait une utilisation merveilleuse du produit des amendes.

M. Nathaniel Erskine-Smith: Merci beaucoup.

Le président: Monsieur Kelly, pour la première intervention de cinq minutes.

M. Pat Kelly (Calgary Rocky Ridge, PCC): Je vous remercie tous d'être ici.

Quand nous avons entrepris l'étude de la Loi sur l'accès à l'information et des systèmes en place, beaucoup de témoins, y compris vous, monsieur Rubin, avez commencé par donner des exemples très convaincants et très éloquents des lacunes que laisserait subsister le statu quo, doublés d'arguments très énergiques sur la nécessité du changement. Dans vos exposés, vous avez soulevé beaucoup d'excellents motifs de préoccupation sur les angoisses des Canadiens au sujet de la protection de la vie personnelle, des changements technologiques et de réalités qui jusqu'ici semblaient du domaine de la science-fiction.

Qu'en est-il de l'argument impérieux sur la nécessité de rédiger à nouveau la loi, par opposition, peut-être, à certaines mesures stratégiques en place? Si chacun de vous prenait une trentaine de secondes pour en parler?

M. Ken Rubin: Dans les sondages et ainsi de suite, beaucoup de répondants classent la protection de la vie privée au premier rang de leurs préoccupations, et je ne crois pas qu'on les rassure. Au dire de beaucoup, la vie privée est chose du passé, mais, d'autre part, il y a un grand besoin d'être rassuré, y compris par la loi. Il faut actualiser la loi pour redonner confiance au public en cette époque où la surveillance rend beaucoup plus difficile la protection de la vie privée. Il a besoin de savoir qu'il existe une certaine rigueur et ainsi de suite. Si on n'invoque pas le pouvoir de maintenir l'ordre, la Charte, d'autres lois, il n'aura pas l'impression qu'on protège son pouvoir d'influence et la vie privée. Nous avons besoin de ce changement.

Mme Brenda McPhail: Le public appelle l'Association pour des questions de vie privée portant notamment sur ce qu'il entend aux nouvelles, par exemple que le Centre de sécurité des télécommunications met des téléphones dans les aéroports sur écoute ou que la police rassemble des milliers de données personnelles pour attraper un voleur de bijoux au moyen d'un dispositif Stingray, et, chaque fois, il demande en quoi ce peut être légal.

Il s'en dégage le sentiment que quelque chose va essentiellement de travers si on ne peut pas comprendre que certaines pratiques qu'on dit légitimes le sont effectivement.

Il éprouve le sentiment que la loi déçoit ses attentes, qu'on devrait limiter la quantité de données qu'on peut collecter sur chacun et utiliser.

Dans mon exposé, j'ai parlé un certain nombre de fois de la confiance. Celle du public dans les organismes qui rassemblent de l'information sur les gens s'érode. Vous pourriez penser que ça concerne peut-être plus le secteur privé, mais la confiance dans l'État est essentielle à la participation à notre société démocratique. Il est absolument essentiel que les citoyens croient que leur gouvernement a leurs intérêts à coeur dans la protection de leurs données personnelles. Sinon, l'approbation sociale dont jouissent les organismes publics comme les agences nationales de sécurité ou les corps policiers sera compromise. Je crois que nous percevons déjà des signes de ce revirement. Ce serait pour moi un exemple convaincant.

● (1225)

M. Tamir Israel: Je ferais en grande partie mienne l'opinion de mes deux collègues et j'ajouterais un exemple de plus, qui attire beaucoup l'attention et qui mine la confiance du public. C'est dans le contexte de la sécurité, où les atteintes à la protection des données sont plus nombreuses et plus fréquentes, souvent de données détenues par l'État. Elles conduisent souvent à des préjudices pour les individus sous forme, souvent, de vol d'identité et d'autres préjudices secondaires. Elles érodent la confiance du public. En toile de fond, c'est de l'information que les citoyens doivent confier au gouvernement pour mener leur vie au quotidien.

Dans ce sous-ensemble particulier de considérations, en plus de celles que mes collègues ont mentionnées, il faudrait imposer et formaliser l'obligation de mesures techniques de sécurité pour que le Bureau du commissaire à la protection de la vie privée déploie toute son expertise dans ce domaine pour nous faire adopter des mesures poussées de sécurité et imposer l'obligation de prévenir à tout coup les victimes de ces atteintes, le cas échéant, pour qu'elles puissent y remédier. Ces problèmes gagneront de plus en plus en importance parce qu'ils deviendront plus complexes, ils ne le deviendront pas moins

Le président: Merci.

Monsieur Saini.

M. Raj Saini (Kitchener-Centre, Lib.): Merci à vous tous d'être ici.

J'ai une observation à faire et je veux connaître votre opinion.

Quand la loi a été rédigée, la première fois, tout se faisait par écrit, et, maintenant, nous passons au numérique. Il subsiste toujours la crainte de rassembler trop de données et de les communiquer à trop de personnes. La loi, actuellement, prévoit que les institutions de l'État peuvent rassembler des données qui, d'après elles, concernent directement le programme qu'elles analysent. L'un des problèmes, et Mme McPhail et M. Israel en ont parlé, c'est la nécessité de collecter l'information.

Comment définiriez-vous un critère de nécessité? Comment pourrions-nous l'insérer dans la loi?

M. Tamir Israel: Nos observations écrites, que nous présenterons en temps voulu, vous donneront des idées pour la loi. Beaucoup de textes provinciaux homologues à la Loi sur la protection des renseignements personnels parlent d'une obligation de nécessité. Cette obligation joue un rôle important. On pourrait parvenir au même résultat avec la norme en vigueur, c'est-à-dire de l'information touchant un programme opérationnel. Mais en orientant la réflexion sur la nécessité, on franchit un pas important qui permet à l'État d'atteindre ses objectifs légitimes mais qui réoriente les pratiques adoptées par les fonctionnaires pour les données en les amenant à réfléchir sur la nécessité réelle de cette information et sur la durée pendant laquelle ils envisagent avoir besoin de la conserver.

En explicitant la nécessité, on aurait une norme légale définie. Elle aiderait aussi à réorienter la réflexion sur certaines habitudes, pour ne pas rassembler trop de données ni les conserver trop longtemps.

M. Raj Saini: Madame McPhail, aviez-vous une opinion?

Mme Brenda McPhail: Je serais d'accord avec M. Israel. Je pense qu'il importe vraiment qu'une disposition de la loi amène les fonctionnaires à se demander non seulement ce qu'ils peuvent collecter, mais ce qu'ils devraient collecter. Est-ce nécessaire? Est-ce important? Voilà les questions à se poser et les modalités techniques pour les introduire.

Si c'est utile, nous pourrions vous communiquer des mémoires, mais le principe général, l'idée prioritaire, en cette époque de collecte outrancière de données, c'est que le gouvernement préconise de se demander d'abord si c'est nécessaire. Je pense que c'est fondamental et vraiment important.

M. Thomas Keenan: Je voudrais parler en faveur de l'offuscation des données, par laquelle on échappe à l'obligation de conserver toutes les données et de les conserver telles quelles.

J'ai été approché par un membre d'un syndicat provincial qui m'a dit que les salaires de ses collègues allaient figurer jusqu'au dernier cent sur la liste de divulgation du salaire des fonctionnaires, au risque de les exposer au vol de leur identité. J'ai répondu que ce risque était vraiment réel. Si quelqu'un s'adresse à une banque en connaissant exactement votre salaire, c'est un autre paramètre de l'identité.

J'ai proposé d'arrondir les montants à 500 $ près. Comme ce n'est pas arrivé, peut-être que, en réalité, l'État n'a pas besoin des données aussi précises qu'il pourrait le penser. Il pourrait utiliser les données dans des fourchettes. Statistique Canada fait un travail admirable pour qu'il devienne impossible de rattacher les données qu'il publie à telle personne. Personne ne semble y songer. Nous semblons toujours croire qu'il faut connaître un montant au cent près. Peut-être que ce n'est pas nécessaire.

M. Ken Rubin: Les lois sont toujours rédigées de manière à prévoir des exceptions à telle ou telle disposition. Pourquoi n'y en a-t-il pas sur ce qui est nécessaire? Je pense qu'une liste des données que le gouvernement n'a pas à dresser pourrait faciliter une définition plus étroite de la nécessité.

● (1230)

M. Raj Saini: Monsieur Israel, je tiens à vous poser une question précise, sur laquelle les autres pourront aussi émettre des observations.

Vous avez écrit sur l'importance de donner avis à l'intéressé d'une atteinte à sa vie privée. Vous en avez parlé. Auriez-vous plus de détails sur le genre de système que ça exigerait. Comment fonctionnerait-il?

M. Tamir Israel: Un régime maintenant adopté dans la Loi sur la protection des renseignements personnels et les documents électroniques, qui pourrait être très efficace aussi dans la Loi sur la protection des renseignements personnels, vise à aviser l'intéressé de l'existence d'un risque de préjudice, et le préjudice est défini d'une façon à entraîner, de la part de l'intéressé, la prise de mesures pour réduire le risque qui permettrait de l'avertir en temps opportun pour qu'il les prenne.

Ça entraîne aussi la nécessité, pour l'institution, de conserver des registres des atteintes même les moins nocives, pour que nous ayons une meilleure idée de celles qui touchent les mesures de sécurité, lesquelles, encore une fois, prendront de l'importance pour que des organismes comme le commissaire à la vie privée ou l'organisme chargé de la cybersécurité puisse examiner le phénomène et en avoir une meilleure idée. Si, faute de registre, chaque organisme ne s'occupe seul que de son petit problème, impossible de se faire une idée globale du phénomène et de faire progresser les normes.

Encore une fois, nous essaierons de traiter plus exhaustivement la question dans notre mémoire. À notre stade actuel de réflexion, le mécanisme qui se trouve dans la Loi sur la protection des renseignements personnels et les documents électroniques donne aussi en gros de bons résultats dans le contexte de la Loi sur la protection des renseignements personnels. Mais nous essayons toujours de voir s'il faut s'occuper de questions propres au secteur public, si ça peut être utile.

Le président: Merci beaucoup, monsieur Saini.

Entendons maintenant M. Kelly, qui dispose de cinq minutes.

M. Pat Kelly: Par suite de ma question antérieure je comprends et j'ai une idée qu'il existe certainement de l'anxiété chez ceux qui sont en contact avec, par exemple, l'Association canadienne des libertés civiles en exprimant leur inquiétude sur les anecdotes qu'on entend et sur la maîtrise des technologies nouvelles et la crainte de leurs conséquences.

Il semble y avoir une plus grande inquiétude du fait de l'évolution des technologies que des exemples d'atteinte à la sécurité de l'information ou des exemples précis de manipulation inadéquate de l'information par l'État.

Qu'est-ce que chacun de vous fait de la recommandation du commissaire pour que son bureau reçoive un mandat explicite de sensibilisation du public en recherche? La sensibilisation sur la vie privée, certains parmi vous, chers témoins, ont discuté de la valeur que les Canadiens accordent ou devraient accorder à la vie privée.

Que faites-vous de la recommandation d'accorder au commissaire un mandat de sensibilisation? Qu'en pensez-vous, rapidement?.

M. Ken Rubin: Je pense que c'est important, mais je pense aussi que l'augmentation de ses pouvoirs d'enquête — c'est son principal travail — est encore plus importante, parce que, actuellement, il ne dispose pas de tous les outils pour s'adresser aux tribunaux ou pour faire des recommandations sur les métadonnées, les données biométriques et tout le reste.

Si vous ne voyez pas d'objection à revenir à ce dont vous parliez plus tôt, voici la loi et demandez-vous pourquoi ça doit se faire pour nous. C'est la disposition sur l'objet de la loi. Elle ne parle pas du droit à la protection des renseignements personnels, mais du droit d'accès aux renseignements personnels, ce qui est totalement différent. Quant aux articles sur la collecte, la conservation et le retrait, ils occupent une page et demie et ne disent rien. Ils sont dépassés.

Je pense que nous devons faire plus que d'accorder au commissaire plus de pouvoirs et plus de pouvoirs explicites. Il s'occupe déjà de sensibilisation et ainsi de suite. Il a besoin de réaliser plus d'audits, de faire plus d'évaluations technologiques.

En ce qui concerne la loi, je pense qu'elle a besoin d'être actualisée, et si je suis sorti du cadre de votre question, vous m'en voyez désolé.

M. Pat Kelly: Pas du tout, c'est très bien.

M. Tamir Israel: Je tiens à dire et à souligner sans ménagements que nous estimons qu'il y a des lacunes sur le plan des enquêtes dans les éléments importants de la loi, auxquelles il faut s'attaquer du point de vue de la politique publique et au sujet desquelles il faudra rassurer le public.

Je pense aussi que l'élément de sensibilisation est important sur ces deux aspects. Nous consacrons beaucoup de temps à expliquer aux gens ce qui arrive. On a parfois tendance à réagir trop ou pas assez, à cause de la très grande complexité de la technologie et de la difficulté d'en comprendre les effets sur le terrain. Un mandat de sensibilisation serait très utile sur ces deux aspects, comme il l'est déjà dans le secteur privé, grâce à la Loi sur la protection des renseignements personnels et les documents électroniques.

● (1235)

M. Pat Kelly: J'ai une question pour M. Keenan.

L'une de vos premières affirmations dans votre préambule sur les pirates informatiques m'a intrigué par la distinction que vous faites entre bons et mauvais pirates. C'est peut-être une appréciation subjective. Si on possède le droit fondamental à la protection de sa vie privée, qu'est-ce donc qu'un bon pirate informatique?

M. Thomas Keenan: À mes yeux, les bons pirates sont ceux qui dévoilent les vulnérabilités et qui en parlent. Un type m'a déjà dit: «Je vais t'expliquer quelque chose.» Environ la moitié des immeubles au Canada sont verrouillés à l'aide de ce qu'on appelle une carte HID. Ce type m'a dit qu'il avait trouvé une façon de pirater ces verrous à distance. Il travaille pour une grande entreprise. Il a révélé cela au fabricant de cette carte, au même titre qu'il y a un an des gens ont mis au jour les vulnérabilités des voitures comme la Jeep Grand Cherokee, qui peut être piratée à distance.

J'ai aussi appris quelque chose d'intéressant. Même si General Motors et d'autres fabricants ont trouvé des solutions pour remédier à ce problème, les principales entreprises de location de véhicules n'ont pas encore mis en place ces solutions. Il est donc possible de louer aux États-Unis une voiture qui peut encore être piratée, car les entreprises de location ne veulent pas perdre de l'argent en retirant ces véhicules.

Ce que je veux dire, c'est que certaines choses doivent être faites. Les pirates nous informent, mais il appartient au responsable des données, ou des voitures dans ce cas-ci, de régler le problème.

Le président: Je vous remercie pour cette réponse.

Monsieur Bratina, vous avez cinq minutes.

M. Bob Bratina (Hamilton-Est—Stoney Creek, Lib.): Je m'intéresse aux conséquences d'une infraction, d'un vol de propriété intellectuelle, de dommages, de la perte de réputation, etc. Nous opposons la notion de méfait à celle de dénonciation. Est-ce que Snowden est un héros ou un vilain?

M. Tamir Israel: Pouvez-vous accorder une amnistie, ou est-ce que cela dépasse votre champ de compétence?

M. Bob Bratina: Nous pouvons le recommander.

M. Tamir Israel: Ayant travaillé dans le domaine avant l'affaire Snowden, je peux vous dire que nous avions prévu un grand nombre des activités qu'il a révélées, et bien des gens ont trouvé qu'elles étaient un peu disproportionnées. Cette révélation a eu à tout le moins le mérite de lancer une sérieuse discussion à propos des paramètres appropriés pour ces activités.

Il n'y avait pas moyen d'obtenir des preuves, même si nous savions ce qui se passait, à l'instar des mauvais acteurs. Il n'y avait pas moyen de provoquer le débat, alors recevoir directement cette information crédible sur ce qui se passait sur le terrain a été utile pour nous en tant qu'organisation de la société civile.

Je crois savoir qu'il a été prudent en s'assurant que l'information qui allait être rendue publique était éditée de façon à ne pas trop nuire aux capacités de sécurité. C'est tout à son honneur, mais chacun est libre d'en juger.

M. Bob Bratina: Monsieur Rubin, avez-vous un commentaire?

M. Ken Rubin: Je crois qu'il nous a rendu un précieux service. Lorsqu'on parle d'élargir le mandat du Commissaire à la protection de la vie privée en matière d'éducation, je crois qu'il faut dire que chacun, que ce soit au travail ou dans le quotidien, doit être vigilant ou demander des comptes à propos de ce qu'il sait et en parler. Ce sont des problèmes auxquels nous sommes tous confrontés, alors je crois qu'il est très important que ce type-là ait exposé toutes ces technologies et qu'il ait confirmé tout cela, car autrement, nous ne le saurions pas.

Je crois qu'il faudrait offrir des incitatifs à ces personnes — appelons-les les dénonciateurs — et une certaine protection aux bons pirates, qui dévoilent ce genre de chose. Nous n'avons pas besoin d'un autre document d'information au sujet des métadonnées. Nous avons plutôt besoin de personnes qui sont aux premières lignes et qui nous disent ce qu'il en est. Il s'agissait d'une importante divulgation.

Si le président Obama veut lui accorder le pardon, je serais d'accord.

M. Thomas Keenan: Je connais les parents de Snowden. Sa mère lui a fait parvenir un exemplaire de mon livre. Je lui ai demandé si elle voulait l'avoir en version électronique, et elle m'a répondu que ce n'était pas nécessaire, car elle pouvait lui faire parvenir des choses en Russie.

Il nous a certainement rendu service, c'est indéniable, et parfois c'est subtil. Par exemple, l'année dernière, le département américain de la Défense a lancé un concours de piratage du Pentagone. Pour participer, il fallait être un véritable pirate américain. Des failles dans le système ont été constatées. Cela prouve que rien ne peut être entièrement sécurisé, et c'est le Pentagone qui l'a admis. Je ne suis pas certain que cet exercice aurait eu lieu s'il n'y avait pas eu l'affaire Snowden.

● (1240)

M. Bob Bratina: Madame McPhail.

Mme Brenda McPhail: À l'instar des autres témoins, je penche davantage pour le héros que le vilain. Ce n'est que lorsque nous avons appris ce qui se passait exactement dans le monde que nous avons amorcé une discussion sur la surveillance de masse, les limites qu'il faudrait fixer ainsi que l'efficacité et l'utilité de cette surveillance.

Je fais partie d'un groupe international de défense des libertés civiles. Je peux vous dire que des gens dans la société civile dans tous les pays utilisent l'information qu'il a divulguée pour amorcer des discussions dans leur société au sujet des limites qu'il convient d'imposer pour la surveillance et l'équilibre qu'il faut atteindre entre le droit à la vie privée et le droit à la sécurité dans les sociétés démocratiques. Je crois qu'il a apporté une contribution très précieuse.

M. Bob Bratina: Je vous remercie, monsieur le président.

Le président: La parole est maintenant à M. Blaikie. Vous disposez de trois minutes, monsieur. Ensuite, monsieur Long, je crois que nous pourrons vous accorder une minute pour terminer vos questions.

Monsieur Blaikie.

M. Daniel Blaikie: Je vous remercie beaucoup.

Je sais qu'on a parlé d'une norme qui existe en Europe. Je me demande si l'un ou l'autre des témoins peut donner d'autres exemples de bonnes mesures législatives sur la protection des renseignements personnels qui sont en vigueur dans d'autres pays, et en particulier mentionner certaines caractéristiques de ces lois qu'il serait judicieux d'adopter au Canada.

M. Thomas Keenan: J'ai parlé du Règlement général sur la protection des données de l'Union européenne. Certaines personnes disent que c'est la raison du Brexit. C'est un document de 88 pages qui énonce des règles. C'est un peu bureaucratique. Je crois qu'il faudrait y trouver les très bonnes idées qu'il contient, et non pas l'adopter tel quel.

M. Tamir Israel: Il existe un certain nombre de documents dans les différents pays. L'OCDE a établi des lignes directrices en matière de protection des renseignements personnels. Le Canada a participé très activement à une mise à jour de ce document il y a un an ou deux. Le Conseil de l'Europe a établi un cadre général comparable pour la protection des renseignements personnels qui s'inspire du cadre européen, mais qui est un peu plus universel et moins détaillé; c'est un document beaucoup moins volumineux. On est en train de le mettre à jour, alors vous devriez surveiller cela.

L'une des recommandations qu'il contient concerne la transparence en ce qui a trait aux décisions prises à l'aide d'algorithmes. J'en ai parlé très brièvement durant mon exposé. C'est un problème qui se posera dans l'avenir, à mesure que les gouvernements utiliseront des processus automatisés pour prendre diverses décisions. Le défi est de faire preuve de transparence en ce qui concerne le processus de prise de décisions sans révéler les calculs. On travaille actuellement à trouver une solution à ce problème, alors il faudra rester à l'affût. Nous pourrions vous donner d'autres exemples par écrit.

Merci.

M. Daniel Blaikie: J'ai une dernière question à propos de quelque chose que je trouve curieux.

Lorsqu'on parle de l'utilisation accrue de la technologie et des données, on peut penser aux partis politiques, qui recueillent beaucoup de données maintenant. C'est une situation qui n'est pas prévue dans la Loi sur la protection des renseignements personnels, parce qu'il s'agit du gouvernement. Elle n'est pas prévue non plus dans la LPRPDE ni dans aucune autre mesure législative. Dans quelle loi conviendrait-il d'ajouter des dispositions concernant l'utilisation des renseignements personnels par les partis politiques?

M. Ken Rubin: Je crois que les lois devraient contenir des dispositions à cet égard.

Je sais que le commissaire à la protection de la vie privée a affirmé qu'il ne s'occupera pas de cela. Toutefois, en Inde, la loi sur l'accès à l'information contient des dispositions visant les partis politiques, car ils recueillent des fonds et détiennent des bases de données assez considérables. Si on envisage d'assujettir à ces lois le secteur privé et certaines organisations qui ne font pas partie du milieu des affaires, il devrait en être de même pour les partis politiques.

Mme Brenda McPhail: Je suis d'accord, et je soulignerais que l'Alberta, qui a commencé récemment à revoir sa Loi sur la protection des renseignements personnels, nous a précisément demandé si cela devrait être inclus dans cette loi, et nous avons répondu que ce devrait l'être.

Les partis politiques recueillent une grande quantité d'information, qu'ils analysent de la même façon que tout organisme des secteurs public et privé peut le faire. Ils l'utilisent à des fins très précises et ils obtiennent des données qui proviennent de sources auxquelles les citoyens peuvent ne pas avoir pensé. Toute cette information mérite d'être protégée convenablement. Peut-être que des dispositions à cet égard devraient être incluses dans LPRPDE, d'autant plus que le commissaire à la protection de la vie privée a affirmé qu'il ne pense pas que des dispositions devraient être ajoutées à la Loi sur la protection de la vie privée.

J'encourage le Comité à réfléchir à quelle loi il estime que des dispositions devraient être incluses, et à les ajouter.

● (1245)

Le président: Je vous remercie beaucoup.

Monsieur Israel, allez-y rapidement.

M. Tamir Israel: Je dirais brièvement qu'il pourrait y avoir des chevauchements, car parfois, une partie de l'information est transmise du gouvernement aux partis politiques. Cette situation pourrait être visée par la Loi sur la protection des renseignements personnels et tout le reste par la LPRPDE. Cela mérite d'être envisagé.

Le président: D'accord, je vais remercier nos témoins.

Chers collègues, nous allons faire une pause de quelques minutes, et ensuite les 15 dernières minutes de la séance se dérouleront à huis clos. Je vais demander à nos témoins de quitter la salle le plus rapidement possible. Je tiens à vous remercier très sincèrement. Nous avons eu d'excellents échanges aujourd'hui, et nous vous en sommes reconnaissants. Je sais que si nous avons d'autres questions, nous pourrons communiquer avec vous.

Je vous remercie beaucoup pour votre contribution.

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