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 042 • 1re SESSION • 41e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 31 mai 2012

Président

M. Pierre-Luc Dusseault

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

Le jeudi 31 mai 2012

● (1100)

[*Français*]

Le président (M. Pierre-Luc Dusseault (Sherbrooke, NPD)): Bonjour à tous. Bienvenue à cette deuxième réunion du comité où nous entendons des témoins à propos de notre étude sur la protection des renseignements personnels et les médias sociaux.

J'ai le plaisir de souhaiter la bienvenue à Mme Scassa, à M. Geist et à Mme Steeves, tous trois de l'Université d'Ottawa. Ils vont faire une présentation et ils disposent de 10 minutes chacun. Ensuite, il y aura une période de questions et réponses au sujet des présentations qui auront été faites.

Sans plus tarder, je donne la parole à la personne qui veut commencer.

Madame Scassa, allez-y.

Mme Teresa Scassa (chaire de recherche du Canada en droit de l'information, Faculté de droit, section de common law, Université d'Ottawa): Merci beaucoup de m'avoir invitée à vous parler aujourd'hui.

Je vais faire mes commentaires en anglais, mais je serai heureuse de répondre aux questions en anglais ou en français.

[*Traduction*]

J'aimerais commencer par préciser que je pense qu'il est très important d'accorder plus d'attention à la protection des données et à la vie privée en lien avec les activités des entreprises de médias sociaux. Je trouve un peu ironique que le mandat du comité soit d'étudier les mesures et les efforts adoptés par les entreprises de médias sociaux pour protéger les renseignements personnels des Canadiens. C'est un peu comme si on étudiait les efforts déployés par les renards pour protéger les poules.

Je remarque que les efforts déployés par Google, Facebook et d'autres entreprises de médias sociaux pour tenter de protéger les renseignements personnels des Canadiens ont été orientés par les lois sur la protection des données. Il faut donc veiller à ce que ces lois soient adéquates.

Les modifications découlant du premier examen quinquennal, en 2006, n'ont pas encore été adoptées par le Parlement; de plus, le deuxième examen quinquennal accuse déjà un retard. On devrait s'en inquiéter, surtout parce que l'environnement de la protection des données a beaucoup changé depuis que la loi a été adoptée.

Il est difficile de faire respecter la loi actuelle. En effet, la commissaire n'a pas le pouvoir d'adopter des arrêtés et ne peut pas infliger des amendes ou d'autres pénalités dans le cas d'un comportement particulièrement inapproprié.

À mon avis, la discussion sur les médias sociaux et la vie privée présente deux volets. Le premier concerne la façon dont les gens utilisent ces outils pour communiquer entre eux. À ce sujet, on nous a fait part de préoccupations à l'égard des employeurs qui consultent les pages Facebook, des personnes qui affichent dans Internet les renseignements personnels d'autres personnes, des criminels qui exploitent les renseignements affichés sur Facebook, etc. Ce sont des préoccupations concernant les renseignements que les gens ont choisi de divulguer, les conséquences de cette divulgation, et les normes qui devraient régir ce nouveau mode de communication interpersonnelle.

Le deuxième volet, sur lequel je vais me concentrer, concerne le rôle de ces entreprises dans la cueillette ou dans la facilitation de la cueillette de grandes quantités de renseignements à notre sujet dans le but de suivre nos activités en ligne, nos habitudes de consommation et même nos déplacements. À cet égard, il est important de porter notre attention sur de grandes entreprises, par exemple, Facebook et Google, mais il existe aussi un grand nombre d'autres joueurs qui adoptent ces pratiques dans l'environnement numérique.

En général, les modèles opérationnels des entreprises de médias sociaux dépendent beaucoup des données personnelles de leurs utilisateurs. En fait, le réseautage social, les moteurs de recherche, les courriels et de nombreux autres services nous sont offerts gratuitement. En hébergeant nos contenus et en suivant nos activités, ces services sont en mesure d'extraire une quantité importante de données personnelles. La nature et la qualité de ces données sont constamment améliorées à l'aide d'innovations. Par exemple, les renseignements concernant l'emplacement des personnes et leurs déplacements sont très prisés. De plus en plus de gens possèdent des téléphones intelligents qui indiquent leur position; ils utilisent ces appareils à des fins de réseautage social et pour d'autres activités en ligne. Même les navigateurs d'ordinateur sont maintenant géo-dépendants, et des renseignements sur l'endroit où nous sommes sont recueillis régulièrement lorsque nous naviguons dans Internet.

Il s'ensuit que de plus en plus de données de toutes sortes sont recherchées, recueillies, utilisées et divulguées. Ces données sont compilées, comparées et étudiées afin d'établir le profil des consommateurs pour différentes raisons, y compris le marketing axé sur le comportement. Dans certains cas, ces données peuvent être communiquées à des entreprises de publicité, à des développeurs d'applications ou à d'autres entreprises connexes. Même lorsqu'on dépersonnalise les données, leur nature précise peut tout de même permettre d'identifier la personne concernée; des entreprises comme AOL et Netflix l'ont appris à leurs dépens.

Les renseignements détaillés des profils permettent aussi d'identifier les personnes. L'énorme quantité de renseignements recueillis à notre sujet nous rend très vulnérables à tous les types de manquement à la sécurité des données. Il devient très difficile de protéger nos renseignements personnels, surtout lorsque les préférences de confidentialité sont souvent établies par défaut par des services que nous utilisons quotidiennement ou même plusieurs fois par jour, par exemple, Facebook ou un moteur de recherche.

Il est souvent difficile de déterminer quels renseignements sont recueillis, et comment et à qui ils sont communiqués. Les politiques de protection de la vie privée sont souvent trop longues, pas assez claires et trop éloignées des gens pour qu'ils puissent les lire et les comprendre. De nos jours, nous effectuons quotidiennement une série de transactions et nous n'avons tout simplement pas le temps ou l'énergie de gérer nos données de façon appropriée. C'est un peu comme marcher dans un marais et se retrouver dans un nuage de moustiques. Pour les empêcher de nous piquer, nous pouvons agiter les bras; nous pouvons même utiliser des insecticides ou d'autres dispositifs, mais au bout du compte, ils vont nous piquer — souvent à plusieurs reprises.

Il est aussi de plus en plus difficile d'éviter d'entrer dans ce marais. En effet, les gens utilisent les médias sociaux afin de resserrer les liens avec leur famille et leurs amis, peu importe à quelle distance ils vivent, ou parce que les médias sociaux font partie intégrante de la façon dont leur groupe communique et interagit. Les entreprises, les écoles et même les gouvernements sont de plus en plus présents dans les médias sociaux, ce qui pousse encore plus les gens à s'aventurer dans ces environnements. Les fournisseurs de contenu traditionnel exercent maintenant leurs activités sur Internet, Facebook et Twitter, et encouragent leurs lecteurs, et ceux qui les écoutent et qui les regardent à obtenir leurs nouvelles et d'autres renseignements en ligne et dans des formats interactifs. Ces outils remplacent rapidement les moyens de communication traditionnels.

● (1105)

À ce jour, notre protection principale contre l'exploitation de nos renseignements personnels dans ces contextes a été fournie par les lois sur la protection des données. Ces lois sont fondées sur la nécessité de trouver un équilibre entre la vie privée des consommateurs et le besoin des entreprises de recueillir et d'utiliser des données personnelles; toutefois, depuis que la LPRPDE a été adoptée, les entreprises sont devenues insatiables en ce qui concerne ces données, et elles les conservent pendant plus longtemps. Autrefois, on avait besoin de ces renseignements pour compléter des transactions ou pour maintenir la relation avec le client, mais aujourd'hui, on les considère comme une ressource à exploiter. Ce changement risque d'éviscérer le modèle de consentement sur lequel la loi est fondée. Ce nouveau paradigme mérite une attention particulière et pourrait nécessiter des normes et des approches juridiques différentes.

Le modèle traditionnel de protection des données visait à permettre aux consommateurs d'effectuer des choix éclairés au sujet de leurs renseignements personnels. Dans le contexte général des données, il est très difficile de faire des choix éclairés. De plus, il y a un élément de servitude qui est très perturbant. Nancy Obermeyer utilise l'expression « géo-esclavage volontaire » pour décrire un contexte dans lequel les dispositifs géo-dépendants communiquent constamment nos déplacements à de nombreuses entreprises sans que nous en soyons nécessairement conscients. À son avis, équiper les personnes avec des capteurs qui envoient des renseignements sur leurs activités les rend vulnérables à la dominance et à l'exploitation — pourtant, c'est de plus en plus une réalité dans nos vies quotidiennes. Au-delà de la simple cueillette de données, les services de réseautage social encouragent leurs utilisateurs à faire de ces sites le centre de leurs activités et de leurs communications quotidiennes.

Nos données personnelles sont une ressource que les entreprises, peu importe leur taille, exploitent régulièrement. Ces renseignements sont utilisés pour établir notre profil, afin de définir nos habitudes de consommation, de déterminer si nous nous qualifions pour des assurances ou d'autres services, ou d'exercer une discrimination fondée sur le prix lors de la livraison de marchandises ou de services. Nous devenons des personnes concernées dans tous les sens du terme. Il existe peu de transactions ou d'activités qui ne laissent pas de traces sous forme de données.

Comme on l'a souligné plus tôt, un grand nombre de services dits gratuits, par exemple, les sites de réseautage social, les sites d'échange de documents, les applications et même les moteurs de recherche Internet, sont en fait fondés sur la capacité d'extraire les renseignements personnels de l'utilisateur. En 2011, dans l'affaire St. Arnaud c. Facebook, un juge de la Cour supérieure du Québec a refusé d'autoriser un recours collectif contre Facebook, car il aurait fallu établir que les conditions d'utilisation du site constituaient un contrat de consommation, de façon à ce que les lois du Québec puissent déroger à la clause selon laquelle tous les conflits seraient réglés en vertu des lois de la Californie et devant les tribunaux californiens. La Cour du Québec a décidé qu'il ne s'agissait pas d'un contrat de consommation, car les services de Facebook sont gratuits, alors qu'un contrat de consommation est fondé sur le principe qu'il y a un paiement et une contrepartie. Le juge a décidé que les utilisateurs n'avaient pas d'obligations qui pourraient représenter une forme de contrepartie.

L'affaire démontre à quel point la divulgation de renseignements personnels est négligée dans un contrat entre une entreprise et une personne. On suppose qu'il s'agit seulement d'un élément régi par les politiques tangentielles sur la protection de la vie privée. Ce manque de transparence à l'égard de la contrepartie fait en sorte que les consommateurs assument l'entière responsabilité de la gestion de leurs renseignements personnels.

On peut donc réfuter les préoccupations concernant le fait que des quantités excessives de renseignements personnels sont recueillies en affirmant que les gens ne se préoccupent tout simplement pas de leur vie privée. Par contre, lorsqu'on considère que l'échange de renseignements personnels constitue un élément d'un contrat de consommation visant des services, on ne peut plus écarter les lois sur la concurrence et les préoccupations concernant la protection des consommateurs. À mon avis, il est temps de s'occuper concrètement de ces préoccupations.

Les grandes bases de données peuvent occasionner un autre dommage social; il s'agit bien sûr de la discrimination. D'ailleurs, Oscar Gandy en parle dans son plus récent ouvrage. Nous comprenons comment le profilage fondé sur la race mène à des injustices lors de l'application des lois criminelles. Qu'il soit fondé sur la race, le sexe, l'orientation sexuelle, la religion, l'ethnicité, le statut socioéconomique ou d'autres éléments, le profilage engendre de plus en plus de préoccupations concernant la façon dont on nous offre des biens ou des services. Grâce aux renseignements personnels, les entreprises établissent le profil de nos goûts et de nos habitudes de consommation. Ils nous les renvoient par le biais d'annonces publicitaires taillées sur mesure, de recommandations et de promotions. Lorsque nous cherchons des biens et des services, on nous présente d'abord les choses qu'on croit que nous voulons.

On nous dit que le profilage est une bonne chose, car cela signifie que nous ne serons pas bombardés d'annonces publicitaires faisant la promotion de produits ou de services qui nous laissent indifférents. Pourtant, l'autre côté de la médaille, c'est que le profilage peut être utilisé pour déterminer que des personnes ne sont pas admissibles à des rabais ou à des prix promotionnels, qu'elles ne se qualifient pas pour du crédit ou des assurances, ou qu'il est sans intérêt de les viser par le marketing d'un type particulier de produits et de services. Le profilage peut exclure certaines personnes et en privilégier d'autres, et c'est ce qui va se produire.

J'ai fait valoir que les grandes bases de données modifiaient le paradigme de protection des données et que les services de réseautage social, ainsi qu'un grand nombre d'autres services Internet gratuits, jouaient un rôle de premier plan à cet égard. Pour terminer, j'aimerais me concentrer sur les points suivants.

Tout d'abord, la cueillette, l'utilisation et la divulgation de renseignements personnels ne concernent plus seulement la protection de la vie privée, mais ces activités soulèvent aussi, entre autres, des questions relatives à la protection du consommateur, aux lois sur la concurrence et aux droits de la personne.

● (1110)

Deuxièmement, la nature et la quantité de renseignements personnels recueillis par les sites de médias sociaux et d'autres services gratuits sur Internet vont au-delà des renseignements nécessaires aux transactions et concernent plutôt les activités, les relations, les préférences, les intérêts des personnes et l'endroit où elles se trouvent.

Troisièmement, la réforme de la Loi sur la protection des données n'a que trop tardé, et elle pourrait maintenant nécessiter une reconsidération ou une modification de l'approche fondée sur le consentement, surtout dans les contextes où les données personnelles sont traitées comme une ressource et que la cueillette de ces renseignements s'étend aux déplacements, aux activités et aux intérêts.

Quatrièmement, les modifications à la LPRPDE devraient inclure de plus grands pouvoirs de mise en oeuvre en ce qui concerne les normes de protection des données, ce qui pourrait signifier le pouvoir de prendre des ordonnances et d'infliger des amendes ou des pénalités aux cas d'infractions graves ou de récidives.

Ceci termine mon exposé. Merci beaucoup.

[*Français*]

Le président: Merci beaucoup.

Monsieur Geist, vous disposez de 10 minutes.

[*Traduction*]

M. Michael Geist (titulaire de la Chaire de recherche du Canada, droit d'Internet et du commerce électronique, Université d'Ottawa, à titre personnel): Merci beaucoup.

Bonjour, je m'appelle Michael Geist. Je suis professeur de droit à l'Université d'Ottawa et titulaire de la Chaire de recherche du Canada en droit d'Internet et du commerce électronique. J'ai été membre du groupe de travail national sur le pourriel créé par le ministre de l'Industrie en 2004, et je siège actuellement au conseil consultatif d'experts du Commissariat à la protection de la vie privée du Canada. Toutefois, je comparais aujourd'hui devant votre comité à titre personnel et je ne représente que ma propre opinion.

Dans mon exposé, je définirai plusieurs avenues quant aux mesures que le gouvernement pourrait prendre, mais je souhaite fournir un bref contexte et trois mises en garde.

Premièrement, il s'agit peut-être d'une lapalissade, mais je préciserai que les médias sociaux représentent une innovation hautement importante aux retombées positives. Le nombre d'utilisateurs est en forte croissance; l'importance de cette technologie comme principale source pour les activités de communication, les activités communautaires et les activités politiques s'accroît de jour en jour. À mon avis, il faudrait profiter des occasions qu'offrent les médias sociaux, plutôt que les démoniser. De plus, le gouvernement devrait travailler activement à intégrer les médias sociaux dans ses processus de consultation en matière de politiques.

Deuxièmement, dans une certaine mesure, le Canada a été un chef de file dans l'utilisation et la réglementation des médias sociaux. La commissaire à la protection de la vie privée du Canada a été la première à mener une importante enquête sur la protection de la vie privée par Facebook. Ses travaux ont mené à l'examen d'autres questions touchant les médias sociaux et les fournisseurs de services Internet.

Troisièmement, nous avons exercé une certaine influence dans le cadre de ces enquêtes, mais le Canada n'a pas joué un rôle de premier plan dans la création des services de médias sociaux utilisés par des millions de personnes à l'échelle mondiale. Je crois que le fait de ne pas avoir énoncé et mis en oeuvre une stratégie nationale en matière d'économie numérique revient nous hanter; notre capacité d'apposer un sceau résolument canadien sur les médias sociaux est minée par nos manquements politiques. En effet, le Canada a déployé très peu d'efforts pour encourager la création de sites de commerce et de médias sociaux canadiens.

Dans ce contexte, que pouvons-nous faire? J'aimerais vous exposer quatre avenues.

Tout d'abord, je pense que nous devons terminer ce que nous avons entrepris.

Le gouvernement a proposé et adopté des dispositions législatives qui pourraient être utiles pour traiter certains enjeux découlant de l'utilisation des médias sociaux. Pourtant, ces initiatives n'ont pas atteint leurs objectifs. Par exemple, le projet de loi anti-pourriel, qui avait reçu la sanction royale en 2010, n'est toujours pas entré en vigueur, car la version définitive du règlement n'a pas été approuvée. En fait, selon les représentants d'Industrie Canada, le règlement n'entrera probablement en vigueur que plusieurs mois après le début de 2013. Étant donné la somme de travail investie dans ce projet, je trouve qu'il est scandaleux que la loi ait été laissée en suspens.

De plus, le projet de loi C-12, projet de réforme de la LPRPDE qui visait à apporter des modifications découlant de l'examen sur la protection de la vie privée de 2006, traîne à la Chambre des communes, car il ne semble y avoir aucun intérêt pour le faire avancer. En fait, je dirais qu'il est maintenant désuet et qu'un examen complet de la LPRPDE sur de nouveaux enjeux, par exemple, le pouvoir de prendre des ordonnances — comme vous venez de l'entendre —, les dommages-intérêts et le resserrement des exigences d'établissement des rapports sur les manquements à la sécurité en fonction des exigences définies dans le projet de loi, est devenu nécessaire. En fait, les règles du projet de loi C-12 sur l'établissement de rapports en matière de manquement à la sécurité n'ont pas assez de mordant en raison de l'absence de pénalités pour défaut de s'y conformer.

Depuis des années, les différents gouvernements promettent une stratégie en matière d'économie numérique, et ils n'ont pas respecté leur engagement. La stratégie est maintenant connue sous l'appellation « le dossier Penske », nom qui fait référence à l'épisode de l'émission*Seinfeld* où l'on travaillait à un dossier imaginaire. Tandis que d'autres pays s'attachent depuis plusieurs années à la mise en oeuvre de leur stratégie, le Canada est toujours en retard sur ce plan.

À mon avis, il faudrait aussi souligner que ces questions doivent de plus en plus être traitées de concert avec les provinces. La frontière entre les compétences fédérales et provinciales n'est pas claire dans bon nombre de cas et les contestations juridiques de la loi fédérale constituent un risque réel. Des efforts devront être déployés pour commencer à élaborer des normes minimales pouvant être mises en application au niveau provincial, au cas où le leadership fédéral ferait l'objet de contestations devant les tribunaux par des sociétés cherchant à contourner leurs obligations en matière de protection de la vie privée.

Deuxièmement, le diable est dans les détails. À de nombreux égards, les médias sociaux et les fournisseurs de services Internet sont les plus puissants décideurs quand il est question de choix en matière de protection de la vie privée. Comme le dit mon collègue Ian Kerr, le diable est dans les détails. En d'autres mots, les choix faits par les plus grandes sociétés de médias sociaux quant aux paramètres par défaut en matière de protection de la vie privée sont les choix par défaut pour des millions d'utilisateurs. Étant donné la pression grandissante en vue de la création de revenus, nous pouvons nous attendre à ce que ces choix par défaut subissent des modifications considérables visant à permettre une utilisation optimale des données d'utilisateur.

Certaines sociétés effectuent pourtant de l'excellent travail dans ce domaine. Ainsi,Twitter a mis en place dernièrement des options de non-suivi qui ont été louées par la Commission fédérale du commerce aux États-Unis. De même, Google offre à ses utilisateurs des outils de transparence grâce auxquels ils peuvent obtenir des renseignements détaillés sur la nature et l'utilisation des données recueillies et sur la façon dont ils peuvent modifier certains de leurs choix en matière de protection de la vie privée. La société a également fait preuve de transparence quant aux demandes d'exécution de la loi pour des demandes de renseignements et de retrait de droit d'auteur.

Il faut déployer des efforts soutenus à l'égard des paramètres par défaut, élaborer des initiatives visant à fournir aux utilisateurs davantage d'information et de transparence et prendre des mesures pour faire en sorte que les sociétés respectent leurs engagements en matière de protection de la vie privée.

● (1115)

Troisièmement, il y a la question de l'accès légal. Le dépôt du projet de loi C-30 sur la surveillance d'Internet a déclenché une avalanche de préoccupations et une forte indignation dans la population. Le projet de loi s'attache en grande partie à la divulgation obligatoire sans mandat de renseignements sur les abonnés par les fournisseurs de services de télécommunications, mais il ne faut pas négliger la possibilité que les médias sociaux et les sites Internet affichant de grandes quantités de données servent à peu près le même objectif.

Une enquête menée dernièrement par le Commissariat à la protection de la vie privée au sujet du réseau social canadien Nexopia a révélé l'existence de centaines de demandes d'exécution de la loi pour des noms et adresses de clients, souvent liées à des comptes qui auraient dû être supprimés plusieurs mois auparavant. Les médias sociaux, comme nous l'avons entendu, créent une mine de renseignements personnels qui doivent être entièrement protégés et faire l'objet d'une surveillance par les tribunaux avant leur divulgation. En effet, selon des documents obtenus dernièrement en vertu de la Loi sur l'accès à l'information, Sécurité publique étudie la façon dont les règles s'appliquent aux sites et aux services des médias sociaux. À mon avis, le projet de loi C-30 devrait être retravaillé de sorte à tenir compte efficacement de ces enjeux.

Quatrièmement, il y a la question des nouveaux enjeux juridiques, dont certains ont été soulevés par Mme Scassa. Je pense que de nombreuses mesures peuvent être prises pour utiliser ou renforcer les règles existantes, mais les médias sociaux et Internet soulèvent certaines questions toutes particulières qui pourraient exiger des réponses ciblées. Faute de temps, je vais vous en présenter seulement deux.

Tout d'abord, il y a l'option de non-suivi. Comme vous le savez peut-être, il est possible d'utiliser des témoins pour suivre les habitudes de navigation sur le Web des utilisateurs, y compris lorsqu'ils visitent les sites de tiers. Par exemple, Facebook place un témoin dans les navigateurs des utilisateurs qui font le suivi des activités de navigation sur Internet. Dans le cas de tous les sites qui comportent un bouton de type Facebook, comme les sites des conservateurs, des néo-démocrates et des libéraux, Facebook enregistre chaque visite sur le site et conserve l'information pendant des mois. Un nombre croissant de sites, dont Yahoo, AOL et Twitter, respectent la fonction du navigateur Firefox qui permet à l'utilisateur de choisir de ne pas être suivi. Google a déclaré qu'elle mettrait en place une technologie semblable dans son navigateur Chrome.

Toutefois, de nombreux sites ont été lents à adopter la fonction de non-suivi et Facebook a jusqu'ici refusé de le faire. Étant donné que l'industrie n'a pas réussi à s'autoréglementer, il est justifié que le gouvernement intervienne en adoptant des mesures rigoureuses pour garantir le respect du choix de l'utilisateur.

Deuxièmement, il existe un problème de plus en plus grave de mauvaise utilisation des médias sociaux. Ainsi, au cours des derniers mois, on a recensé un nombre grandissant de cas d'employeurs qui avaient demandé aux candidats à un poste de leur fournir leur code d'identification et mot de passe Facebook s'ils voulaient obtenir une entrevue d'emploi. Il aurait été habituellement interdit par la loi de demander les mêmes renseignements au moyen de questions directes; cette pratique est donc utilisée comme moyen pour contourner les normes et principes de longue date du droit du travail. En réponse à cette pratique, l'État du Maryland a adopté une loi qui interdit aux employeurs d'exiger de leurs employés ou des candidats à un poste de donner l'accès à leur compte personnel de médias numériques ou sociaux. Plusieurs autres États travaillent à l'élaboration d'une loi semblable, et je pense que le Canada devrait leur emboîter le pas.

Merci beaucoup de votre attention.

● (1120)

[*Français*]

Le président: Merci, monsieur Geist.

La parole est maintenant à notre dernier témoin d'aujourd'hui, Mme Steeves, qui dispose de 10 minutes.

[*Traduction*]

Mme Valerie Steeves (professeure associée, Département de criminologie, Université d'Ottawa): Merci beaucoup.

Je suis l'enquêteure principale du projet de recherche de MediaSmarts intitulé Les jeunes Canadiens dans un monde branché. Depuis 12 ans, nous recueillons des données sur les expériences des jeunes concernant la vie privée en ligne, ce qui signifie que nous avons recueilli des données pendant toute la durée de vie de la LPRPDE. Pendant ce temps, nous avons répertorié des changements importants qui, à mon avis, fournissent un contexte important au travail que votre comité s'est engagé à accomplir. J'aimerais donc commencer mon exposé en parlant brièvement de ces changements et je vous présenterai ensuite quatre recommandations concrètes.

En 2000, lorsqu'on a adopté la LPRPDE, on pensait qu'elle mettrait en place des mécanismes d'infrastructure qui encourageraient les gens à faire confiance au commerce électronique, afin qu'ils participent à cette nouvelle façon de créer de la richesse. Lorsqu'elle a été adoptée, nous avons parlé aux parents et à leurs enfants. Les parents à qui nous avons parlé étaient très enthousiastes au sujet de ce projet. Ils étaient convaincus qu'Internet allait être bénéfique à leurs enfants, et que les entreprises qui mettaient au point ces technologies leur donnaient les outils nécessaires pour approfondir leur expérience éducative et les préparer au marché du travail de l'avenir.

Ils nous ont aussi confié qu'ils faisaient confiance au bon jugement de leurs enfants lorsque ces derniers naviguaient sur Internet, et qu'ils n'allaient pas les surveiller continuellement. Ils allaient plutôt rester en retrait. Ils se disaient que leurs enfants feraient quelques erreurs, mais que lorsqu'ils auraient des problèmes, ils demanderaient de l'aide. Lorsque nous leur avons demandé s'ils envisageaient de surveiller leurs enfants lorsqu'ils navigueraient sur Internet, ils nous ont dit que cela minerait la relation de confiance qu'ils entretenaient avec eux. Ils pensaient que s'ils agissaient ainsi, ils ne respecteraient pas la vie privée de leurs enfants, et qu'ils ne le feraient donc pas.

De leur côté, les jeunes à qui nous avons parlé en 2000 jugeaient qu'Internet était un espace complètement privé. Les adultes ne pouvaient même pas le trouver, et encore moins le contrôler. À cette époque, ils ne se préoccupaient pas de la protection de la vie privée en ligne, car ils étaient convaincus que l'anonymat était garanti sur Internet. Ce qui est intéressant, c'est que lorsque venait le temps de décider où aller lorsqu'ils naviguaient sur Internet, ils cherchaient des marques de commerce, car ils pensaient que les entreprises qui possédaient ces marques étaient dignes de confiance. Elles étaient perçues comme des amies et ils pouvaient leur faire confiance.

En 2004, les parents s'étaient certainement rendu compte qu'Internet n'était plus une panacée, mais une source de conflits familiaux. Ils savaient que leurs enfants pouvaient divulguer des renseignements personnels en ligne, et que cela représentait un problème. Ils avaient établi des règles sévères dans la maison et dit à leurs enfants de ne pas le faire, mais ils passaient beaucoup de temps à limiter et à gérer les activités de leurs enfants sur Internet, et à se disputer à ce sujet.

Les enfants à qui nous avons parlé en 2004 avaient tout à fait intégré les technologies en ligne dans leur vie personnelle, ce qui, à mon avis, nous ramène aux commentaires de M. Geist au sujet des avantages des médias sociaux. Les jeunes utilisent ces médias et continuent de s'en servir pour essayer différentes identités, pour approfondir leurs rapports avec leurs amis du monde réel, et pour rechercher leurs propres intérêts. En 2004, ils le faisaient parfois de façon anonyme, mais la plupart du temps, ils souhaitaient divulguer leur identité, car contrairement à la croyance populaire, ils ne parlaient pas à des étrangers. Ils parlaient aux autres jeunes qui fréquentaient leur école et ils devaient s'identifier, afin de trouver leurs amis lorsqu'ils étaient en ligne.

Même s'ils savaient qu'on pouvait les épier et qu'ils utilisaient des soi-disant médias publics, ces jeunes trouvaient tout de même que la protection de la vie privée en ligne était extrêmement importante. Je dirais qu'il faut être prudent lorsqu'on affirme que les jeunes ne se soucient pas de la protection de la vie privée parce qu'ils affichent les détails de leur vie sur Facebook. Ceux qui disent cela n'ont tout simplement pas pris le temps de parler aux jeunes; ils se préoccupent énormément de la protection de la vie privée en ligne. Ils commençaient à s'inquiéter de plus en plus en 2004, et dans un sondage de suivi effectué auprès de 5 500 écoliers canadiens, environ la moitié des jeunes commençaient à remarquer que des publicités s'affichaient sur Internet et qu'elles étaient intégrées aux sites sur lesquels ils naviguaient.

Revenons à 2011. Aujourd'hui, les parents nous disent que parce que les jeunes ont accès à Internet par l'entremise de plusieurs points d'entrée ou de dispositifs — les ordinateurs portatifs, les ordinateurs des laboratoires d'informatique, les réseaux de bibliothèques, les iPod, les téléphones intelligents, les iPad, les consoles de jeux vidéo —, il devient de plus en plus difficile de surveiller leurs activités en ligne. Ils nous ont aussi dit que c'était un très gros problème et qu'ils devaient exercer une plus grande supervision, car la divulgation de renseignements personnels est maintenant inévitable; vous allez en ligne parce que c'est ce qu'on attend de vous. Ils étaient fâchés contre les entreprises en ligne, car à leur avis, elles encourageaient leurs enfants à tout divulguer, dans le but de réaliser un profit. Ce ressentiment et ce manque de confiance sont des changements importants comparativement à 2000, lorsqu'on croyait que les entreprises de haute technologie bâtissaient un avenir dans lequel les jeunes pourraient tirer profit de la technologie.

● (1125)

Pendant cette même période, les sites d'entreprises, surtout ceux qui ciblent les enfants, ont cessé de parler de vie privée pour parler de sécurité. C'est logique du point de vue des entreprises, car lorsqu'elles parlent de la vie privée, elles représentent le risque, étant donné qu'elles recueillent vos renseignements. Par contre, si elles parlent de sécurité, elles peuvent dire aux enfants et à leurs parents de ne pas s'inquiéter, car elles surveillent les enfants et vont veiller à leur sécurité.

Il est intéressant de remarquer que presque tous les parents à qui nous avons parlé en 2011 étaient obnubilés par ces discussions sur les dangers en ligne. En fait, ils avaient tellement peur, qu'ils ont affirmé que de bons parents ne pouvaient plus faire confiance à leurs enfants et ne pouvaient plus se permettre de leur accorder une certaine liberté comme c'était le cas en 2000. Et encore une fois, ils étaient nombreux à jeter le blâme sur les entreprises en ligne. Comme l'un des parents de Toronto l'a dit: « Je suis très contrarié par la peur que ces entreprises ont provoquée chez les gens. » Tous les parents ont dit qu'ils n'étaient même pas certains de la nature de ces dangers. Tout ce qu'ils savaient, c'est qu'ils avaient très peur. Ils ne veulent pas épier leurs enfants, car cela nuirait à leur relation avec eux, mais s'ils doivent le faire pour assurer leur sécurité, ils le feront.

Les jeunes, quant à eux, étaient déjà au courant. Ils nous ont dit que l'espace privé non réglementé dont ils profitaient tellement en 2000 et en 2004 était maintenant complètement surveillé, et qu'ils savaient qu'il était surveillé par les parents, par les écoles, par leurs pairs et par les entreprises qui possèdent les sites qu'ils visitent.

Cela met les jeunes en mauvaise position, précisément parce que les technologies de réseau sont tellement intégrées à leurs interactions sociales. Il est intéressant aussi de souligner que les jeunes ont dit que tout ce dont ils avaient besoin, c'était d'un espace pour parler avec leurs amis. Ils veulent que les parents et les adultes soient à l'arrière-plan, mais ils ont besoin d'intimité pour pouvoir profiter des avantages que procurent les interactions sociales.

Plusieurs d'entre eux ont commencé à parler de délaisser Facebook et d'utiliser leur téléphone cellulaire, car ils se sentaient trop surveillés. Ils ont tous dit que la surveillance dont ils faisaient l'objet par toutes ces personnes différentes minait les liens de confiance qui étaient essentiels pour obtenir l'aide dont ils avaient besoin lorsqu'ils en avaient besoin.

Ils commencent aussi à se demander ce qui va arriver maintenant que les employeurs et la police peuvent avoir accès à leur profil Facebook. Ils commencent aussi à s'inquiéter au sujet des gens sournois à la solde des entreprises qui les surveillent. Lorsque vous entendez des jeunes parler de gens sournois, prêtez l'oreille. Cela signifie que quelqu'un n'a pas respecté les normes et a envahi leur vie privée.

La situation devient compliquée lorsqu'une entreprise agit ainsi, car si un individu louche âgé de 40 ans vous envoie un message sur Facebook, vous le bloquez simplement ou vous l'éliminez de votre liste d'amis. Toutefois, les jeunes nous ont dit qu'ils ne pouvaient pas faire cela avec les entreprises, car ces dernières possèdent les sites qu'ils visitent. Ils pensaient aussi que les politiques en matière de vie privée étaient délibérément rédigées dans un langage tout à fait incompréhensible, afin que les entreprises n'aient pas à révéler comment elles allaient utiliser les renseignements personnels obtenus.

Même si les jeunes ont toujours tendance à se rassembler sur ces sites d'entreprises, par exemple, Facebook et YouTube, ils ne considèrent plus que les entreprises sont amicales ou dignes de confiance. Je pense qu'il est important de ne pas l'oublier, car la LPRPDE a été conçue pour créer ce niveau de confiance.

Que pouvons-nous faire? Comment pouvons-nous améliorer les choses? J'ai quatre solutions à vous proposer.

Tout d'abord, nous devons accroître la transparence des plans d'affaires de ces sites. En 1999, lorsque plusieurs d'entre nous ont comparu devant les membres précédents de votre comité, le gouvernement a dit que la LPRPDE était un seuil minimum, et non un plafond. Aussitôt qu'elle a été adoptée, la loi est rapidement devenue un plafond.

J'aimerais préciser qu'il existe de nombreuses preuves qui démontrent que les mécanismes de consentement sur lesquels nous nous fondons, ainsi que les conditions d'utilisation et les politiques en matière de vie privée, ne sont pas rédigés dans le but de permettre aux gens d'effectuer des choix éclairés sur les renseignements qu'ils divulguent; ils sont rédigés pour protéger des poursuites judiciaires l'entité qui recueille ces renseignements.

De plus, il devient de plus en plus difficile de savoir comment ces renseignements sont utilisés. J'aimerais vous donner deux brefs exemples à ce sujet.

En 2000, j'ai fait beaucoup de recherches sur un site appelé Neopets, qui permet aux jeunes de créer un animal de compagnie en ligne. Les jeunes doivent gagner des points sur ce site pour pouvoir acheter des produits associés à leur animal, et ils gagnent ces points en répondant à un sondage commercial.

En 2000, le site demandait aux jeunes de répondre à un sondage sur la nourriture qu'ils consommaient au déjeuner, par exemple, et dans ce contexte, on leur a posé des questions supplémentaires, par exemple, combien d'argent font vos parents? Avez-vous une grande maison? Combien d'automobiles votre famille possède-t-elle? Quel type d'automobile vos parents conduisent-ils? On leur a aussi demandé de choisir, parmi 60 intérêts, des choses qui les intéressaient. La liste comprenait des choses comme la bière, l'alcool, les cigares, la cigarette et le jeu. Ces renseignements étaient ensuite utilisés pour intégrer des publicités dans le site, afin d'encourager certains types de consommation

J'ai une idée du plan d'affaires de ce site. Depuis ce temps, en raison des préoccupations qui ont été soulevées au Canada et aux États-Unis, ces pratiques sont devenues beaucoup moins transparentes. Aujourd'hui, je peux seulement avoir accès à ce genre de renseignements par le courrier ordinaire et si je prétends être une entreprise. En ma qualité de chercheuse, de parent et de citoyenne préoccupée, je ne sais plus où m'adresser. Je ne peux pas vous dire ce que les entreprises font avec les renseignements qu'elles obtiennent.

● (1130)

Il est aussi devenu beaucoup plus difficile de savoir comment ces renseignements sont utilisés. La cueillette ne se produit plus sous nos yeux; elle se produit en arrière-plan. J'ai reçu une demande d'amitié de Facebook, même si je n'ai jamais eu de compte Facebook. Je n'ai aucun lien avec cette entreprise. Dans la demande, on précisait qu'il s'agissait de quelqu'un qui s'appelait Melissa et que je voudrais peut-être être amie avec elle, et que je devrais donc joindre leur réseau. Je n'ai jamais eu de liens avec cette entreprise, mais elle a réussi à me retrouver par ma fille, même si nous n'avons pas le même nom de famille, et même si elle n'a jamais eu un compte Facebook. Je n'ai pas divulgué ces renseignements. Je n'ai aucun lien avec cette entreprise, et pourtant, elle est en mesure de tenter de manipuler mon comportement par l'entremise d'une utilisation commerciale qui n'est pas transparente.

Deuxièmement, je vous conseille vivement de ne pas examiner seulement l'utilisation des renseignements personnels...

[*Français*]

Le président: Je vous demanderais de conclure rapidement en nous présentant vos deux dernières recommandations.

[*Traduction*]

Mme Valerie Steeves: D'accord. J'ai presque terminé.

Je vous conseille vivement d'examiner aussi les utilisations des données agrégées, car c'est la façon dont fonctionnent les profils dont parlait Mme Scassa. Les renseignements personnels ne sont pas les seuls problèmes de protection de la vie privée auxquels nous faisons face sur Internet.

Troisièmement, je recommanderais que l'article 3 de la LPRPDE vous donne l'occasion de découvrir les raisons pour lesquelles les données agrégées et les renseignements personnels sont utilisés par les entreprises.

Quatrièmement, lorsque nous discutons de ce sujet, nous concluons souvent qu'il faut éduquer davantage les gens. Après avoir travaillé dans le milieu de l'éducation privé pendant les 18 dernières années, je dirais qu'il est temps de commencer à prendre l'enseignement de la culture numérique au sérieux. En ce moment, parce que le gouvernement ne l'appuie pas, vous la laissez, par défaut, aux entreprises. Nous devons appuyer les organismes d'intérêt public, afin qu'ils puissent fournir aux gens les renseignements dont ils ont besoin pour faire des choix éclairés et prendre des décisions informées en ce qui concerne Internet.

Merci beaucoup.

[*Français*]

Le président: Merci beaucoup. Je remercie les trois témoins.

On passe maintenant à une période de questions et réponses de 10 minutes.

Monsieur Angus, vous pouvez commencer.

[*Traduction*]

M. Charlie Angus (Timmins—Baie James, NPD): Merci beaucoup à tous nos témoins. Cette discussion est fascinante.

Le Nouveau Parti démocratique considère que les nouveaux médias offrent un incroyable potentiel démocratique et de grandes possibilités de développement sur le plan social. La question est de savoir comment atteindre l'équilibre. Certains éléments perturbants se produisent sur le Web 2.1 ou 2.0, et nous devons être prudents. C'est ce qui est important. Nous ne voulons pas trop agir et interférer, mais nous voulons veiller à ce que cette protection existe.

Madame Scassa, je voulais commencer par la question que vous avez soulevée à l'égard de la LPRPDE, car il s'agit de notre première ligne de défense. Notre commissaire à la vie privée a souligné que le Canada accumule un retard de plus en plus grand. Nous sommes peu avancés en matière de protection fondamentale de la vie privée. Je suis inquiet au sujet des exigences de signaler les infractions. Il semble que la refonte potentielle de la LPRPDE permettrait aux entreprises de décider un peu trop librement de divulguer on non à une personne que sa vie privée a été infiltrée. On parle d'un risque grave. La barre est plutôt haute. Je ne peux pas imaginer une entreprise divulguer volontairement à ses consommateurs que quelqu'un a piraté ses données.

Devons-nous imposer le signalement obligatoire? Des sanctions administratives pécuniaires garantiraient-elles que ces entreprises prendront la protection des renseignements personnels au sérieux?

Mme Teresa Scassa: En ce qui concerne les sanctions pécuniaires et le signalement des atteintes à la sécurité des données, l'éventuel établissement de limites à l'obligation de signaler les atteintes à la sécurité ferait problème. En effet, ces atteintes sont malheureusement si fréquentes et si diverses que l'obligation automatique de les signaler toutes accablerait rapidement les consommateurs, qui se méfieraient encore plus de l'utilisation que les entreprises font de leurs données. Dans la diversité des problèmes, il faut trouver un juste milieu, qui se traduit par l'obligation de signaler uniquement les atteintes graves, qui ont vraiment fait courir un risque aux consommateurs ou aux particuliers.

Ce juste milieu, on peut le trouver de plusieurs façons. On peut s'en remettre à l'entreprise pour déterminer la gravité de l'atteinte et la nécessité de la signaler. On peut aussi obliger les sociétés à signaler les atteintes au commissaire à la protection de la vie privée, puis à décider, avec lui, des mesures à prendre pour avertir les consommateurs. Il peut exister toute une gamme d'avertissements ou de réactions.

Dans une certaine mesure, je comprends la crainte de submerger les consommateurs d'avertissements, mais, en même temps, je pense qu'il existe des manières de le faire sans laisser aux seules compagnies le soin de décider du moment où une atteinte présente un risque grave de préjudice.

La notion de risque grave de préjudice est également difficile à cerner, parce qu'il n'est pas toujours facile d'évaluer la gravité du risque de préjudice pour les individus. Ce sera, je pense, un seuil difficile à franchir.

Les sanctions administratives seraient un important moyen dans l'arsenal du commissaire. Non seulement elles punissent les fautifs, ce qui peut être utile pour signaler un comportement problématique auquel il faut remédier, mais elles acquièrent aussi une dimension d'humiliation publique. Je pense que l'un des reproches fréquents contre la Loi sur la protection des renseignements personnels et les documents électroniques est la bonasserie du commissaire pour les fautifs, dont il tait les noms, particulièrement de ceux dont on se plaint le plus, etc., de sorte que l'information est insuffisante.

● (1135)

M. Charlie Angus: Nous sentons indéniablement la nécessité de permettre au commissaire de jouer un rôle d'arbitre, parce que quelqu'un pourrait certainement paniquer à la suite d'une atteinte quelconque, sans nécessairement en connaître la gravité. Le commissaire représente certainement l'intérêt public et il possède les pouvoirs.

Monsieur Geist, je suis curieux au sujet du retard du Canada. Le Canada était un chef de file mondial dans le développement du numérique. Il y a six ou sept ans, c'était ici que l'on observait l'un des taux de pénétration les plus élevés, idem pour l'accès et la vitesse. Aujourd'hui, les normes de l'OCDE nous guident, et nous sommes dans la queue, le dernier tiers, du peloton. Notre vision bornée nous empêche de voir l'objectif et d'imaginer une stratégie du numérique polyvalente, qui tient compte de la participation démocratique, des droits des consommateurs et de l'initiative économique. Pouvez-vous nous expliquer vos motifs de préoccupation?

M. Michael Geist: Volontiers. Voilà qui touche à un enjeu que, à mon avis, la plupart des pays aussi avancés que nous, la plus grande partie des pays développés, ont reconnu comme absolument essentiel à la prospérité économique et à l'innovation à long terme, comme un attribut faisant partie intégrante de notre système d'éducation, de nos modes de divertissement et de notre culture. Il joue tant de rôles différents.

Je pense, comme les derniers mois l'ont révélé, à la faveur du projet de loi C-30, du projet de loi SOPA, aux États-Unis, de l'Accord commercial relatif à la contrefaçon (ACRC), en Europe, qu'il se double également d'une dimension politique et participative très importante.

À cet égard, il ne s'est pratiquement rien fait au Canada, contrairement à la plupart des autres pays, qui ont élaboré des stratégies pour l'économie numérique, en se concentrant sur tous les moyens d'assurer un accès général pour franchir la démarcation, dans le domaine du numérique entre, d'une part, le simple accès aux ordinateurs et, d'autre part, la culture numérique et les aptitudes dont Mme Steeves a parlé et la politique visant à baliser convenablement l'éclosion d'entreprises et leur croissance.

En fait, il y a quelques années, sous la houlette du ministre de l'Industrie — le ministre Clement —, il s'est tenu d'excellentes consultations. Elles ont suscité beaucoup de réactions. Beaucoup de pays pouvaient nous inspirer. Pourtant, on n'a proposé aucune stratégie pour l'économie numérique. On a bien proposé quelques projets de loi, un, notamment, que j'ai mentionné, contre les pourriels, mais dont les règlements sous son régime, 18 mois après la sanction royale, se font encore attendre.

Le dernier budget a notamment vu la suppression de mécanismes comme le programme d'accès communautaire, le PAC, alors que se présentait au moins une occasion de chercher à obtenir une impulsion du secteur privé. Aux États-Unis, le gouvernement et d'importants fournisseurs de services Internet se sont efforcés de fournir des ordinateurs et une connectivité à large bande à bon marché pour procurer un accès aux éléments les plus pauvres de la société. Rien de tel au Canada.

Le comité se demande avec quels grands enjeux stratégiques se colleter. Une partie du problème vient du fait que presque aucune société canadienne marquante n'intègre dans ses activités le genre de valeurs canadiennes dont nous parlons.

Vous avez peu de moyens pour assurer le respect des lois, parce que toutes ces compagnies sont étrangères. Cela ne veut pas dire que vous êtes réduits à l'impuissance totale — nous avons vu qu'on pouvait prendre des mesures — mais nous nous placerions sur un terrain vraiment plus solide si nous nous attelions tout simplement à la tâche d'établir un cadre pour l'avenir.

● (1140)

[*Français*]

Le président: Merci, monsieur Geist.

Monsieur Angus, votre temps de parole est écoulé.

Je cède la parole à M. Del Mastro pour sept minutes.

[*Traduction*]

M. Dean Del Mastro (Peterborough, PCC): Merci, monsieur le président.

Merci aux témoins. Vos exposés ont été très intéressants.

Mardi, le commissaire à la protection de la vie privée a affirmé ici que les données volumineuses étaient une sorte de devise dont les Canadiens se débarrassaient sans contrepartie et sans vraiment comprendre la nature de ce qu'ils cédaient.

Madame Scassa, je pense que vous avez parlé des entreprises qui rassemblent, récoltent, auriez-vous dit, des renseignements sur nous.

Monsieur Geist, vous avez parlé des paramètres par défaut de la protection de la vie privée et du fait que le diable gisait dans les détails.

Madame Steeves, je suis très étonné que vous ayez pu recevoir la suggestion d'un ami par l'entremise de votre fille, qui porte un nom de famille différent du vôtre, sans jamais avoir été inscrite dans Facebook.

Mme Valerie Steeves: Oui.

M. Dean Del Mastro: En fait, c'est assez remarquable. Cela montre bien la quantité de recherche et d'information rassemblée, dont, à mon avis, les Canadiens n'ont pas idée. Lorsque le commissaire à la protection de la vie privée parle de cette devise cédée sans contrepartie, et des paramètres par défaut actuels de la protection des renseignements personnels, on ne devrait pas, je pense, parler de consentement éclairé.

Tous nos témoins, aujourd'hui, sont professeurs de droit. Ils savent ce qu'est une clause de dénégation de responsabilité. Ne serait-il pas logique de commencer par simplifier, de se débarrasser du jargon juridique et d'expliquer au consommateur les conséquences de sa signature et que, si cela ne lui dit rien qui vaille, un clic au bon endroit suffira? Est-ce que ça ne serait pas un bon point de départ?

J'aimerais connaître le fond de votre pensée sur le consentement éclairé. Je pense que la notion de suivi pourrait troubler beaucoup de Canadiens.

Mme Valerie Steeves: Merci.

En fait, j'ai fait de la recherche financée par le bureau du commissaire. Il s'agissait de faire lire à des jeunes les politiques de confidentialité d'un certain nombre de sites qu'ils fréquentaient, pour savoir s'ils pouvaient les comprendre.

Mon adjointe à la recherche a 24 ans. Elle est diplômée universitaire. Elle poursuit des études supérieures. Elle m'a demandé de l'aider à comprendre la teneur d'une politique de confidentialité. Il m'a fallu une journée et demie pour en venir à bout. Pourtant je suis avocate. La politique comportait 17 hyperliens qui conduisaient à autant de sites. Il y avait des contradictions, des lacunes. Ç'a été une expérience phénoménale. Quand les jeunes affirment que c'est vraiment difficile à comprendre, ils ont raison.

Nous avons présenté ces politiques aux jeunes et ils ont répondu par un ensemble de stratégies pour des politiques écrites en un langage clair. Nous avons ensuite comparé le résultat à ce qui avait été publié. Par une coïncidence ironique, c'était exactement la même chose que ce que tous les universitaires proposaient.

Nous avons réécrit les politiques puis nous les avons testées de façon empirique. Nous avons fait une expérience. Nous avons communiqué aux jeunes la version d'origine des politiques, qu'ils comprenaient très peu et nous leur avons également communiqué les versions remaniées, qu'ils comprenaient bien. Nous les avons publiées. Nous avons mis à la disposition des entreprises 10 pratiques exemplaires censées les aider à rédiger leurs politiques de confidentialité, mais elles n'ont pas trouvé preneur.

M. Dean Del Mastro: Pouvez-vous les communiquer au comité?

Mme Valerie Steeves: Certainement. Elles sont accessibles en ligne.

M. Dean Del Mastro: Merci.

Monsieur Geist.

M. Michael Geist: Je crois que je suis un peu déchiré par ce que je vois. Il est indéniable qu'il faut s'assurer que les choix et les politiques proposés sont mieux compris.

Tout d'abord, je ne pense pas, tout à fait franchement, que ces textes sont conçus pour être lus. Même s'ils étaient mieux rédigés, il n'est pas réaliste de croire que les gens s'arrêteront chaque fois pour lire une politique de confidentialité avant de s'inscrire dans un site Web, vu le nombre de sites qu'une personne peut visiter et avec lesquels elle peut réagir et vu la tendance vers les environnements mobiles et sans fil.

Il serait plus réaliste de prévoir des mécanismes comme l'interdiction de suivi pour que, ses choix faits, la personne raisonnable soit susceptible de se trouver bien à l'aise de fournir une certaine quantité de renseignements. Il se peut même qu'elle ne soit pas consciente des conséquences, mais convenons que si elle télécharge une photo ou une liste de ses préférences, elle n'est pas sans savoir que cette information circulera dans le milieu qu'elle aura indiqué. Nous craignons une mauvaise utilisation, l'agrégation, etc., mais la personne possède des connaissances et une liberté de choix.

Ensuite, il y a le suivi de son activité en ligne. Comme j'ai mentionné, presque tous les partis politiques ont mis sur leurs sites des boutons de préférences. Ils mettent à la disposition des visiteurs des boutons de « tweet » pour faciliter le « retweet ». Nous aimons tous ces gadgets, parce qu'ils facilitent nos relations avec notre réseau. En réalité, tous ceux qui se trouvent sur un site Web renvoient en fait uniquement un message qui, tant qu'on se trouve dans Facebook ou Twitter — peu importe le site —, signale à Facebook que telle personne vient de visiter tel site Web.

Je pense que cet espionnage ne correspond pas aux attentes raisonnables de l'utilisateur. Je me méfierais vraiment d'un message suffisamment clair pour amener la personne à se dire d'accord pour qu'on suive à la trace tous les sites Web qu'elle se trouvera à visiter pendant les deux prochains mois, tant que, sur la page, on trouvera une sorte de widget de Facebook.

Nous avons besoin de mécanismes qui offrent des options d'abstention plus faciles. Il en existe, nous en avons vu, mais trop de gros joueurs répugnent à utiliser ces pratiques contraires à certains de leurs modèles d'affaires. Et c'est là que le gouvernement peut intervenir. Si ces joueurs ne veulent pas s'auto-réglementer convenablement, il les y obligera.

● (1145)

M. Dean Del Mastro: Merci.

Mme Teresa Scassa: Je suis d'accord avec les deux réponses. Il faut cependant souligner que nous ne nous trouvons plus dans un environnement où on cède des renseignements personnels en échange de la possibilité d'accomplir une opération particulière. Beaucoup d'entre nous restent en ligne du matin au soir. Nous avons avec nous des téléphones intelligents; pour diverses raisons, nous sommes nombreux à les avoir dotés d'options qui permettent à l'interlocuteur de savoir où nous nous trouvons, qui signalent nos déplacements.

On n'y fait plus vraiment attention. Toutes sortes de programmes différents interagissent les uns avec les autres, et les données sont rassemblées et communiquées dans des contextes où les gens sont si habitués à utiliser ces programmes ou applications, ou à interagir de certaines façons, qu'il n'est plus considéré comme normal ou naturel de consulter les politiques de confidentialité.

Pourtant, il se produit des choses à notre insu, avec lesquelles nous ne serions peut-être pas d'accord, si nous savions, des choses qui, à mon avis, changent les règles du jeu. Le législateur devrait réagir.

M. Dean Del Mastro: Merci.

Je suis...

Le président: Vous pouvez poser une question courte.

M. Dean Del Mastro: J'aimerais qu'on m'éclaire sur la distinction entre données agrégées et données particulières. Il me semble que, au fond, tout le monde s'intéresse aux données agrégées, qui n'entrent pas nécessairement en conflit avec la protection de la vie privée de l'individu. Par exemple, si Google affirme que les gens ayant fait une recherche sur tel sujet ont obtenu telles ou telles réponses parmi les 10 premières, je n'y vois pas une intrusion dans la vie privée. J'y vois des renseignements utiles.

Je pense que les diverses méthodes de suivi pourraient le plus inquiéter les Canadiens.

Pouvez-vous expliquer un peu la différence entre suivi agrégé et suivi particulier?

Mme Valerie Steeves: Volontiers.

[*Français*]

Le président: Je vais laisser une personne répondre assez rapidement.

[*Traduction*]

Mme Valerie Steeves: D'accord. Quand on utilise ces données, on rassemble toutes ces données personnelles. On fait le suivi de tendances démographiques. Ensuite, on répartit les gens en catégories, puis on les traite différemment en fonction de leur catégorie. Plus tôt, quelqu'un a dit que ce type de technologie est très important pour le débat démocratique. On peut utiliser ces catégories quand les gens se sont identifiés, pour modifier l'environnement où ils se trouvent.

Je faisais de la recherche sur le réseau Microsoft. Je n'avais pas décliné mon identité, mais j'étais alimentée en nouvelles du jour. Dès que je me suis inscrite sous l'identité d'une jeune Vancouvéroise de 16 ans — ce que je n'étais pas, vous l'aurez peut-être deviné —, les nouvelles du jour ont été remplacées par des nouvelles sur les célébrités, des publicités sur les régimes et d'autres sur la chirurgie plastique. Ce n'est pas qu'on savait que j'étais Val, la jeune Vancouvéroise de 16 ans; mais on savait à quelle catégorie je correspondais.

Il en découle donc des problèmes de discrimination, comme l'a mentionné Mme Scassa, mais ils sont encore plus insidieux, parce qu'ils modifient l'environnement dans lequel la personne évolue en raison de l'identité et de la catégorie hypothétique à laquelle elle correspond. Cela ne ferait pas partie des protections offertes par la Loi sur la protection des renseignements personnels et les documents électroniques à l'utilisation des renseignements personnels, mais cela pose un problème de taille à la protection de la vie privée, parce que cette pratique morcelle les espaces publics nécessaires au débat démocratique et qu'elle expose les populations vulnérables à la discrimination.

[*Français*]

Le président: Merci.

Monsieur Del Mastro, votre temps de parole est écoulé.

Madame Murray, vous disposez de sept minutes.

[*Traduction*]

Mme Joyce Murray (Vancouver Quadra, Lib.): Merci beaucoup d'avoir exposé au comité vos idées sur les solutions que l'on devrait appliquer.

En vous écoutant, je me suis dit que, de certaines manières, le Canada prenait du retard. En même temps, vu certaines compressions budgétaires, on empêche d'autres organismes de contribuer à ralentir ce processus.

Vu la complexité incroyable du sujet de votre exposé et le risque que différents groupes de pression aient des idées différentes sur la marche à suivre, j'aimerais que vous nous disiez si les outils dont notre gouvernement dispose, les lois et règlements, et qu'il peut renforcer, sont adaptés à la vitesse et au dynamisme actuels du milieu. Ou bien faut-il entièrement repenser les solutions qu'entrevoient le Parlement et le gouvernement pour les adapter rapidement aux risques et aux motifs de préoccupations? C'est une question pas mal générale.

● (1150)

Mme Teresa Scassa: Oui, c'est un milieu très difficile. Une des points dont j'ai parlé — et je crois que M. Geist l'a également soulevé —, c'est que les problèmes sont maintenant si multidimensionnels et complexes qu'on ne peut pas, selon toute vraisemblance, les classer dans une seule catégorie de législation sur la protection des données relevant de la compétence fédérale. Ces questions pourraient comporter d'autres dimensions qui font appel à d'autres régimes, par exemple les lois sur la concurrence, les lois sur les droits de la personne ou même les lois provinciales. Par conséquent, certaines questions pourraient nécessiter une approche plus multidisciplinaire et polyvalente; il ne serait donc pas nécessairement avantageux de s'occuper des questions en vases clos.

M. Michael Geist: J'ai quelques observations à faire à ce sujet. Premièrement, je ne pense pas que ce soit le rôle du gouvernement de prétendre être le nouveau shérif en ville dans le domaine des médias sociaux et de dire: « On va s'occuper de tout ce qui est lié aux choix que font les entreprises privées et les personnes. »

C'est franchement difficile de suivre le rythme des changements. Comme on vient de l'entendre, il arrive parfois qu'on ne soit même pas sûr des modèles d'affaires. Dans certains cas, on ne sait pas s'il y en a un. Alors, je pense qu'il serait insensé que le gouvernement adopte l'approche qu'il connaît, en pensant que cela va régler tous les problèmes. Cela dit, il ne fait aucun doute que le gouvernement et les organismes de réglementation ont un rôle à jouer pour établir des paramètres sur ce qui est acceptable et pour s'assurer que ceux-ci tiennent compte des valeurs chères aux Canadiens sur le plan de la protection des renseignements personnels et de la sécurité, ainsi que de la gamme des différentes questions qui se posent.

Dans un tel contexte, je me sens un peu plus optimiste à l'idée que le gouvernement puisse s'engager dans l'établissement de règles générales. À bien des égards, la LPRPDE a été conçue, du moins au départ, avec les meilleures intentions pour justement essayer d'atteindre cet objectif. Comme Mme Steeves l'a mentionné, nous avons maintenant plus de 10 ans d'expérience, et cette expérience montre qu'il faut adapter la loi. Ce n'est pas comme si on la modifiait toutes les 10 semaines. En tout cas, une période de 10 ans, c'est amplement suffisant pour dire qu'il y a des lacunes dans la loi pour ce qui est de la protection des renseignements personnels, lacunes qui méritent d'être corrigées pour s'assurer que les paramètres généraux liés à certaines de ces activités reflètent mieux les attentes des internautes canadiens.

Mme Joyce Murray: J'ai une autre question connexe. Madame Steeves, vous pourriez peut-être faire des observations sur les deux.

On a mentionné qu'on essayait de trouver le juste milieu entre la protection des renseignements personnels et l'accès aux données, ce qui est très important pour les entreprises et les questions en matière de compétitivité. J'aimerais que vous nous parliez des répercussions positives et négatives de cette situation sur les petites entreprises — et non pas les grandes entreprises de collecte de données.

J'aimerais également savoir s'il y a un pays qui dispose d'un cadre pour régler ces questions et qui pourrait être un modèle convenable pour le Canada, ou si nous devons plutôt tenir compte des valeurs et principes propres au Canada et adopter une approche à la canadienne.

Mme Valerie Steeves: Comme on l'a dit tout à l'heure, les questions en matière de protection des renseignements personnels en ligne s'inscrivent vraiment dans la lignée de préoccupations plus générales concernant le marketing, la citoyenneté, les droits de la personne, l'interaction sociale, la démocratie, le dialogue démocratique, et j'en passe. Tout au long de l'histoire de la protection des données, les gens ont toujours cru que ce serait la dernière étape. C'est l'approche du seuil minimum, et non du plafond. On supposait qu'il y aurait des mécanismes par lesquels les gouvernements interrogeraient les fins auxquelles les renseignements étaient utilisés pour déterminer si ces pratiques étaient dans l'intérêt du public. Le cas échéant, nous donnerons alors le feu vert. Ce n'est qu'à ce moment-là que nous utiliserons des pratiques équitables de traitement de l'information pour prévoir des recours, si jamais quelque chose se produit.

Selon moi, la dépendance aux pratiques équitables de traitement de l'information repose probablement sur l'idée naïve qu'une telle mesure sera suffisante. C'est peut-être une condition nécessaire, mais ce n'est pas suffisant.

Ce sont surtout les pays européens qui ont abordé ces questions selon une perspective générale et qui ont trouvé des solutions qui tiennent compte les intérêts généraux liés aux droits de la personne. En Europe, la protection des renseignements personnels est assurée selon une approche axée sur les droits de la personne, et il y a des mesures solides de protection des droits de la personne en ce qui concerne le respect de la vie privée et l'inviolabilité de la personne. Il y a un certain nombre de cas en Islande et en Allemagne où les tribunaux ont pu trouver des solutions créatives, déterminer les fins auxquelles ces renseignements sont utilisés et les soumettre à une sorte de jugement public grâce à des concepts plus vastes.

Je suis d'accord avec M. Geist au sujet du consentement. Le consentement ne sera jamais la solution. C'est, selon moi, une pièce importante, quoique petite, du casse-tête. Il nous faut un autre mécanisme pour demander des précisions sur ces utilisations générales. C'est pourquoi je vous ai parlé de l'article 3 de la LPRPDE.

On a déjà fait valoir devant les membres précédents de votre comité que l'article 3 était nécessaire parce qu'ainsi, on pourrait examiner les utilisations et dire qu'une personne raisonnable ne les estimerait pas acceptables dans les circonstances. Le cas échéant, on ne devrait pas le permettre. Cette disposition vous donne beaucoup de pouvoir parce que vous devez penser plus attentivement à la possibilité de restreindre certaines utilisations des renseignements.

● (1155)

M. Michael Geist: On se pose souvent la question suivante: « Qui s'en sort mieux que nous ou qui est le meilleur, et pouvons-nous l'imiter? »

Lorsque la LPRPDE est entrée en vigueur pour la première fois, je pense que beaucoup de gens croyaient que c'était la meilleure pratique. La loi ressemblait beaucoup à ce qu'on trouvait en Europe et aux États-Unis. À bien des égards, elle essayait d'intégrer les deux approches différentes. Il y a peut-être des divergences de vue sur la question de savoir si des rajustements auraient pu être apportés ici et là, mais la loi visait vraiment cet objectif.

Plusieurs pays considéraient le Canada comme un modèle à suivre; on respectait certains des points de vue européens sur la protection des renseignements personnels, tout en tenant compte des considérations commerciales et des éléments liés à l'application de la loi aux États-Unis.

Toutefois, je dirais qu'au cours des 10 dernières années, nous avons vraiment pris du retard. L'Europe a adopté, à certains égards, des mesures plus rigoureuses relativement à certaines de ces questions, mais nous ne lui avons pas emboîté le pas. Quant aux États-Unis, bien franchement, ils s'en sortent beaucoup mieux que nous dans le domaine de l'application de la loi. On impose là-bas des sanctions réelles. Si quelqu'un commet une infraction du point de vue de la protection des renseignements personnels aux États-Unis, il ne s'en tirera pas en toute impunité. On trouve aussi, au niveau des États, des exigences liées à la divulgation obligatoire des atteintes à la sécurité. Comme je l'ai dit, on a également entamé une transition vers l'interdiction de suivi. Le mauvais usage des médias sociaux, dont j'ai déjà parlé, est également visé.

À mon avis, il s'agit de choisir certaines des meilleures dispositions qui existent, sur le plan de l'application de la loi aux États-Unis et des valeurs ailleurs dans le monde, afin de créer un environnement tel que d'autres pays se mettent à imiter le Canada, plutôt que l'inverse. Au cours de la dernière décennie, nous n'avons pas réussi à définir une loi en matière de protection des renseignements personnels qui suit le rythme de ce monde en pleine mutation.

[*Français*]

Le président: Merci.

Madame Murray, votre temps de parole est écoulé.

Je cède la parole à M. Butt pour sept minutes.

[*Traduction*]

M. Brad Butt (Mississauga—Streetsville, PCC): Merci beaucoup, monsieur le président.

Merci d'être ici aujourd'hui. J'ai trouvé vos trois exposés tout à fait excellents.

Mes filles sont âgées de 12 et 8 ans. Celle de 12 ans a décidé qu'elle aime Twitter, contrairement à M. Angus. Elle a créé son petit compte Twitter, qu'elle utilise pour envoyer des messages, surtout à ses camarades d'école.

En tant que parent, je m'inquiète de la possibilité qu'on puisse accéder, d'une façon ou d'une autre, à des renseignements personnels.

D'après vous, pouvons-nous ou devrions-nous envisager des mesures de protection des renseignements personnels pour les mineurs qui sont différentes de celles prévues pour les adultes? Faut-il présumer que les adultes devraient faire preuve de plus de discernement? Après tout, les adultes sont des adultes et ils devraient agir de façon plus intelligente et plus avisée.

À votre avis, devrions-nous envisager de renforcer les dispositions relatives à la protection des renseignements personnels afin de protéger les mineurs qui utilisent les médias sociaux ou devrions-nous plutôt traiter tout le monde de la même manière, peu importe leur âge?

Mme Teresa Scassa: On pourrait peut-être commencer par Val.

Mme Valerie Steeves: Volontiers.

Dans le cadre du premier examen de la LPRPDE, on avait recommandé d'établir un mécanisme de consentement à plusieurs niveaux qui reconnaîtrait les différences d'âge. L'idée était d'interdire aux entreprises de recueillir des renseignements auprès des enfants en bas d'un certain âge. Puis, à mesure que les enfants grandiraient, ils pourraient adhérer à des programmes permettant aux entreprises d'avoir accès à ces renseignements et à leur envoyer des publicités. Toutefois, cette approche imposait des contraintes réelles quant à ce qu'on serait en mesure de faire. La recommandation peut-être la plus importante était celle d'établir une sorte de bouton « effacer » pour que tous ces renseignements soient oubliés dès que le jeune atteint l'âge de 18 ans.

Si on regarde la façon dont les enfants utilisent la technologie, on constate qu'ils s'en servent pour répondre à leurs besoins de développement. Quand je parle à des enfants de 11 ans, je me sens très soulagée. Ce sont eux qui paraissent les plus matures. Ils disent qu'ils ne participent pas aux réseaux sociaux, certainement pas de façon générale, parce que c'est pour les jeunes plus âgés. Ils sont très conscients des risques, et ils se débrouillent très bien pour les éviter.

Quand ils atteignent l'âge de 13 ou 14 ans, ils passent par une autre étape de développement. En pleine quête d'identité, ils se définissent par les rôles qu'ils jouent. Voilà pourquoi ils ont tendance à faire les quatre cents coups pendant quelques années.

Puis, une fois rendus à l'âge de 15 à 17 ans, jusqu'à la vingtaine, ils explorent leur identité au moyen des réseaux sociaux. Selon leur point de vue, ces technologies sont formidables parce qu'elles leur permettent de répondre à leurs besoins, pendant qu'ils forgent leur individualité et passent à l'âge adulte.

Je ne voudrais certainement pas que les textes que j'ai écrits quand j'avais 14 ans paraissent dans un environnement public. Alors oui, pour les enfants, on a certes besoin d'un bouton « effacer ». Le contexte est certainement différent quand on est mineur.

Une des conclusions intéressantes de la recherche, c'est la croyance que les enfants de l'ère numérique soient différents de nous. Ironiquement, quand ils atteignent l'âge de 29 ans, ils commencent à agir comme vous et moi, et ils utilisent la technologie de la même manière que nous. Ils grandissent, en d'autres mots.

Alors oui, ils sont différents. Je partage les mêmes préoccupations quant à l'utilisation du consentement comme mécanisme pour assurer cette protection parce que nous devons établir un âge pour que ce système fonctionne.

J'ai lancé hier une recherche auprès d'un groupe de jeunes, et un jeune de 11 ans a expliqué au réseau CBC comment tous ses amis du même âge, en sixième année, avaient des comptes Facebook. Ils savent qu'il faut avoir au moins 13 ans, mais il suffit de cliquer sur le bon bouton. À mon avis, on ne rend pas service aux enfants si on leur dit qu'on va les surveiller pour s'assurer qu'ils ont l'âge minimal requis. Cela n'aidera pas. En tout cas, on peut imposer des restrictions d'ordre général qui reconnaissent que les enfants sont des enfants et qui interdisent de recueillir leurs renseignements pour ensuite les utiliser à des fins particulières une fois qu'ils seront grands...

Pensons, par exemple, à la plainte déposée contre le site Nexopia. Il s'agit du réseau social le plus populaire chez les enfants. Une des recommandations de la commissaire était que le site ne conserve pas des renseignements pendant une certaine période. Nexopia s'est contenté de dire:« Désolés, nous les gardons. Il y a beaucoup d'argent dans cette affaire. » On parle de jeunes de 12, 13 et 14 ans.

L'autre facteur est l'utilisation des renseignements. Je n'ai pas le temps d'entrer dans les détails, mais je peux parler de certaines études que nous menons auprès de jeunes filles. Le site est rempli de publicités qui utilisent des images très stéréotypées, particulièrement sur le plan des rôles sexuels. Je viens de faire une recherche qualitative vraiment fascinante auprès de jeunes femmes. Elles parlent de la façon dont ces images viennent limiter leur potentiel, chose qu'elles essaient constamment de refuser. Ces images rétrécissent leur champ de possibilités, au lieu d'élargir leurs horizons.

Oui, nous devons aborder la question différemment quand il s'agit des enfants. Je crois que, pour ce faire, il faut examiner les fins auxquelles l'information est utilisée et déclarer qu'il n'est pas raisonnable de recueillir des renseignements auprès d'enfants de huit ans et d'utiliser ensuite ces données pour essayer de leur vendre quelque chose.

● (1200)

M. Brad Butt: Allez-y.

M. Michael Geist: Mme Steeves étant la spécialiste en la matière, je n'aime pas adopter une position différente. Toutefois, je dois dire que des efforts ont été déployés aux États-Unis pour essayer de cibler les jeunes, sur le plan de la protection des renseignements personnels, grâce à la COPPA, la loi sur la protection des renseignements personnels en ligne des enfants, qui prévoit des mesures de protection précises, notamment la surveillance et le consentement parental pour les enfants de moins de 13 ans. Cette mesure législative est une farce.

Mes enfants ont en fait presque le même âge que les vôtres, et j'en ai un de plus que vous. Ils baignent dans ce monde, eux aussi. L'idée qu'une entreprise dise: « Attendez un peu, on ne va pas recueillir vos renseignements jusqu'à ce que vous ayez le consentement de vos parents. On ne va rien recueillir... »

La vérité, c'est qu'il y a la pression des pairs. Les jeunes désirent être là. Bien franchement, cet environnement comporte aussi beaucoup d'aspects positifs.

L'idée que nous puissions établir des règles précises qui interdisent aux entreprises de recueillir ces renseignements ou qui les obligent à obtenir un consentement plus solide existe depuis presque 10 ans. Il y a eu une tentative législative aux États-Unis. Pour ma part, je pense que c'est un échec lamentable parce que les jeunes sont assez intelligents pour savoir qu'ils peuvent contourner ces règles s'ils le veulent; quant aux entreprises, elles ferment les yeux, même si elles savent que c'est ce qui se produit.

Selon moi, relativement à ces questions, nous avons besoin de normes rigoureuses et exécutoires. Il faut donner à la commissaire à la protection de la vie privée le pouvoir réel de rendre des ordonnances, avec la possibilité d'imposer des sanctions si les gens dépassent les limites. Et cela s'appliquerait à tout le monde.

M. Brad Butt: Merci.

Il ne me reste sûrement plus de temps. Cela doit faire cinq minutes.

Le président: Il vous reste une minute.

M. Brad Butt: C'était la principale question que je voulais poser. Je vais laisser la minute qui reste à quelqu'un d'autre qui souhaite l'utiliser, parce que je vais devoir partir de toute façon.

M. Blaine Calkins (Wetaskiwin, PCC): J'accepte volontiers.

Monsieur Geist, j'ai écouté ce que vous avez dit tout à l'heure. Une de vos observations concernait les attentes raisonnables des utilisateurs quant à la façon dont leurs renseignements personnels pourraient être traités. Cela avait l'air d'une définition juridique. Cette notion est-elle définie quelque part dans la loi en vigueur? Faut-il la définir, ou la définition est-elle dépassée? Est-elle désuète dans la LPRPDE? S'agit-il d'une définition jurisprudentielle?

Il me semble que ce soit une sorte de libellé standard utilisé dans l'industrie, et j'aimerais obtenir plus de précisions à ce sujet.

● (1205)

M. Michael Geist: C'est un jargon qu'emploie l'industrie, que je considère comme hautement problématique. Il est vrai que j'y ai recouru, mais un problème se pose quand on compte sur les attentes raisonnables de respect de la vie privée, comme on le voit régulièrement dans des causes relatives au travail et d'autres affaires où il est question d'attentes raisonnables. Si des politiques en matière de renseignements personnels stipulent que l'on ne devrait s'attendre à aucune protection à cet égard et que l'on a été clairement été avisé que certains vont recueillir tous les renseignements qu'ils peuvent pour tenter d'en tirer profit — ce n'est habituellement pas indiqué de façon aussi claire, mais souvent, c'est essentiellement ce qu'on veut dire —, alors si l'on se demande à quelle protection des renseignements personnels on peut s'attendre, la réponse s'apparente à la célèbre réplique de Sun Microsystems: « Vous n'avez aucune protection, autant vous y faire ». En pareil cas, on ne peut raisonnablement s'attendre à bénéficier d'une protection quelconque parce qu'on a été avisé qu'il n'y en a aucune. Autant s'y faire.

Ainsi, quand on fixe des limites et des normes adéquates, et s'assure qu'on dispose d'outils efficaces pour les appliquer, on rompt avec le paradigme voulant que l'on a que ce à quoi on s'attend et que l'on ne peut s'attendre à tout avoir, pour signifier qu'il existe, au contraire, des normes minimales indiquant ce qui est convenable, et que l'on a des outils pour en assurer la mise en oeuvre et l'application.

[*Français*]

Le président: Merci.

Je donne la parole à Mme Borg pour une période de questions et réponses de cinq minutes.

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

J'aimerais aussi remercier les témoins de s'être déplacés aujourd'hui. On a entendu des témoignages intéressants et on est en train d'ouvrir une boîte de Pandore remplie d'enjeux et de questions.

Ma première question s'adresse à Mme Steeves.

Vous avez dit que quand vous étiez une jeune fille de 16 ans, il y avait des publicités qui s'adressaient spécifiquement à une jeune fille de 16 ans. Pouvez-vous préciser quel effet la publicité sur les réseaux sociaux a sur le comportement des jeunes internautes?

[*Traduction*]

Mme Valerie Steeves: L'un des problèmes qui se posent pour répondre à cette question, c'est le manque de transparence. J'aimerais avoir beaucoup plus d'information sur le plan d'affaires de ces sites, certainement en ce qui concerne le fonctionnement du moteur arrière. Je serais ensuite mieux en mesure de répondre.

Je peux toutefois vous dire ce que je sais sur le moteur avant. On réalise beaucoup de recherches sur la manière dont les gens réagissent aux images que montrent les médias par rapport au sexe, par exemple. Peut-être pourrais-je mieux vous expliquer ce qu'il en est en vous donnant l'exemple de l'initiative eGirls, un autre projet de recherche auquel j'ai participé. Les jeunes femmes nous disent que quand elles vont sur ces sites, elles sont bombardées d'images de filles très minces, hypersexualisées, dont l'identité semble principalement axée sur leur relation avec un homme. Pour jeter les bases de nos travaux, nous avons entrepris une analyse environnementale, examinant 1 500 profils publics que des filles vivant visiblement dans la région d'Ottawa avaient publiés sur Facebook. Il s'agissait de profils publics; nous n'avons pas examiné de profils privés.

Sachez que tous ces profils, à l'exception d'un seul, reprenaient l'image stéréotypée de la femme: de jeunes femmes hypersexualisées, faisant la moue en bikini et ne parlant que de leur copain.

Aucune étude quantitative n'établit de relation de cause à effet entre le marketing et de tels comportements. On présume, comme le font certainement les entreprises de marketing, que ces images sont utilisées parce qu'elles influencent le comportement, ce qu'elles semblent faire fort efficacement. Nous savons cependant, d'après nos échanges avec les jeunes qui vivent dans ces environnements, que ces images très stéréotypées sont de véritables nuisances. Les jeunes femmes qui adhérent à ces images et qui cherchent à s'y conformer se désolent de ne pas pouvoir y parvenir et de ne pas réussir à être aussi mince malgré tous les régimes qu'elles s'imposent. Celles qui aspirent à être quelqu'un d'autre affirment qu'elles sont constamment confrontées à ces images et qu'elles doivent s'en prémunir. Tout cela vient du message de marketing qu'on leur envoie.

Ce qui est intéressant quand on observe l'évolution de la situation au Canada — et Michael a raison de dire que nous avons été des chefs de file dans toutes sortes de domaines —, c'est le grand succès qu'a remporté le programme Rescol. Nous avons offert aux jeunes des endroits publics où ils pouvaient échanger, des lieux neutres qui n'avaient rien de commercial. Le gouvernement fédéral a abandonné le programme peu après l'adoption de la LPRPDE. À défaut d'avoir ce programme, un grand nombre d'organisations soucieuses de protéger les intérêts des jeunes se servent de sites officiels pour intervenir.

Par exemple, nous avons beaucoup travaillé avec des enseignants récemment, et un grand nombre d'écoles disent qu'elles utilisent Google Documents. Rien ne semble indiquer que l'information soit recueillie, utilisée et modifiée pour manipuler les jeunes qui se servent de cette plateforme. Sincèrement, je ne crois pas que mes enfants devraient faire leurs devoirs dans un magasin, vous savez?

Selon moi, le marketing et la publicité comportementaux sont conçus pour ne pas avoir l'air de publicité. Ainsi, si on demande aux jeunes de nous dire ce qu'est Facebook, ils répondent que c'est un réseau social. Ce n'est pas un réseau social: c'est un laboratoire de recherche, mis en place pour recueillir de l'information sur les gens et s'en servir pour leur proposer quelque chose.

Cet outil est d'une efficacité redoutable. Nous avons observé, dans ma recherche notamment, une évolution de la réaction des jeunes à ces images. Je vous référerai à toutes les recherches publiées sur les problèmes relatifs à l'image corporelle et le recours accru à la modification de photos. Les conséquences sont nombreuses. À cet égard, j'ai assisté récemment à une réunion à Edmonton, où se sont réunis des médecins et des universitaires qui considèrent qu'il s'agit d'un problème de santé.

● (1210)

[*Français*]

Mme Charmaine Borg: Je vous remercie. Je suis désolée, il me reste peu de temps et je veux poser une autre question. Cependant, je vois vraiment à quel point la privatisation est en train de réduire l'espace public sur Internet. Je trouve cela très inquiétant.

Ma dernière question, madame Scassa, porte sur le phénomène suivant. Vous avez dit qu'on était en train d'utiliser un langage relatif à la sécurité et non pas spécifique aux renseignements personnels. Pour vous, comment cela change-t-il la relation entre l'internaute, l'utilisateur d'Internet, et les compagnies de réseaux sociaux?

Le président: Il vous reste environ une minute pour répondre à la question.

Mme Teresa Scassa: Je ne sais pas si je comprends bien la question. Parlez-vous du langage de sécurité?

Mme Charmaine Borg: On utilise un langage basé sur la sécurité, par exemple la cybercriminalité, au lieu de concentrer le débat sur le langage entourant les renseignements personnels. Ma question porte sur le changement sémantique.

Mme Teresa Scassa: Il y a certes beaucoup de préoccupations en ce qui concerne la fuite des renseignements personnels dans ces entreprises et la répercussion que cela a sur nous, qu'il s'agisse du vol d'identité ou de la criminalisation d'activités sur Internet.

Les lois sur la protection des renseignements personnels s'appuient toujours sur des renseignements personnels. En réalité, je crois qu'on perd la notion de ce concept, de ce qu'est un renseignement personnel. On reconnaît que c'est le nom, l'adresse, et d'autres renseignements qu'on peut donner à quelqu'un. Mais de plus en plus, un renseignement personnel, c'est un renseignement qui porte sur toutes nos activités, sur tout ce qu'on fait sur Internet et même dans d'autres contextes.

Compte tenu de cela, je crois que nous devons mettre l'accent sur cet ensemble de renseignements personnels que nous partageons de plus en plus avec différentes entreprises. Je ne sais pas si cela répond à votre question.

Le président: Merci.

Madame Borg, votre temps de parole est écoulé.

Je cède donc la parole à M. Mayes, qui dispose de cinq minutes.

[*Traduction*]

M. Colin Mayes (Okanagan—Shuswap, PCC): Merci, monsieur le président. Je remercie également les témoins de nous donner leur avis aujourd'hui.

Monsieur Geist, vous avez évoqué les valeurs canadiennes. En ce qui concerne les renseignements personnels, c'est comme tracer une ligne dans le sable. Ma conception de renseignements personnels pourrait être différente de celle de quelqu'un d'autre. Il y a consentement, mais est-ce que chaque utilisateur peut consentir à aller jusqu'à un certain point et pas plus loin, définissant ainsi son propre consentement? Voilà la difficulté quand on élabore un règlement. Quelles valeurs canadiennes choisit-on, puisqu'elles peuvent varier d'une personne à l'autre? Pourriez-vous préciser un peu votre pensée?

M. Michael Geist: Vous avez raison d'affirmer que les avis sont partagés à cet égard. Je crois toutefois qu'une solution facile se présente. Nous pourrions commencer en nous assurant que les choix personnels en matière de consentement sont respectés et que les organisations qui recueillent l'information dévoilent les renseignements de façon adéquate. Il importe que les gens donnent un consentement éclairé.

Nous devons aller plus loin dans cette direction. Je crois qu'il est juste de dire qu'à l'heure actuelle, le droit canadien ne suffit pas à la tâche. Les atteintes à la sécurité ne sont pas dévoilées et ne font pas l'objet de sanction. Nous n'avons pas le pouvoir d'émettre des ordonnances pour assurer la stricte conformité ni d'imposer des sanctions si cette conformité est inadéquate. Pour le moment, si une entreprise n'aime pas la décision de la commissaire à la protection de la vie privée du Canada, elle dit à cette dernière de s'adresser aux tribunaux, car elle ne respectera pas sa décision. Dans les provinces, les commissaires ont le pouvoir d'émettre des ordonnances et d'appliquer la loi.

Il est difficile de croire que la commissaire à la protection de la vie privée a la capacité de défendre l'intérêt public et d'appliquer les valeurs qui ont largement cours dans la société. La commissaire vous a indiqué qu'elle ne peut accomplir son travail, puisque la loi, qui date de plus de 10 ans, ne lui accorde pas de moyens adéquats pour l'appliquer et que les entreprises sont de plus en plus prêtes à s'opposer à ses décisions.

On s'inquiète du flou qui existe entre les compétences fédérales et provinciales. Mais à la lumière de la décision que la Cour suprême du Canada a rendue en décembre dernier au sujet du règlement sur les valeurs mobilières, je crois que si on ne modifie pas vraiment la loi, quand la commissaire fédérale tentera d'appliquer plus énergiquement les règles, les entreprises qui n'aiment pas sa façon de faire lui diront d'intenter des poursuites. Elles feront traîner les choses pendant des années devant les tribunaux. Ces derniers risquent clairement de dire non ou de conclure que la loi est inconstitutionnelle. Si nous ne faisions rien de plus que de tenter d'assurer une divulgation adéquate et une application convenable du consentement, nous serions loin d'où nous sommes actuellement, compte tenu des lacunes que comporte la loi.

● (1215)

M. Colin Mayes: Voilà une question qui m'intéresse: l'application. C'est comme les chiens qui aboient quand la caravane passe. Réussirez-vous un jour à rattraper la technologie et la manière dont on l'utilise? C'est un défi.

Madame Scassa, la loi s'appliquera-t-elle après qu'une plainte a été formulée? Comment traitez-vous avec ces entreprises? Comment les surveillez-vous? Il en coûte terriblement cher d'affecter du personnel à cette tâche. Ne pouvez-vous réagir que lorsque vous recevez une plainte? Pourriez-vous nous proposer des manières d'appliquer les règles élaborées ici?

Mme Teresa Scassa: La LPRPDE comprend actuellement un mécanisme de plaintes, mais la commissaire a aussi la possibilité de faire des vérifications sur les pratiques des entreprises en matière de renseignements, ce qu'elle a d'ailleurs fait à plusieurs reprises. On peut accorder un éventail de pouvoirs à un commissaire pour procéder à des vérifications ou mettre en oeuvre un processus de plainte, qui pourraient notamment lui permettre de tenir des audiences ou de lancer un processus de son propre chef quand il semble y avoir un problème, par exemple.

On peut agir de toutes sortes de façons sans nécessairement attendre le dépôt d'une plainte. Les mécanismes reposant sur les plaintes sont problématiques, car ils nous obligent à réagir aux plaintes que les gens nous exposent et, comme vous l'avez souligné, ils peuvent s'avérer fort coûteux. Chose certaine, le volume de plaintes a augmenté avec les années; il y a donc d'autres moyens de donner à la commissaire le pouvoir de réagir.

Nous avons déjà parlé du pouvoir d'imposer des amendes ou de prendre des mesures extraordinaires dans des cas particuliers. L'éventail de possibilités est très large, et les lois peuvent offrir bien des solutions. On peut instaurer toute une gamme de pouvoirs, selon les circonstances, la norme ou les préoccupations qui s'appliquent.

[*Français*]

Le président: Merci.

Votre temps de parole est malheureusement écoulé, monsieur Mayes.

Monsieur Boulerice, vous disposez de cinq minutes.

M. Alexandre Boulerice (Rosemont—La Petite-Patrie, NPD): Merci, monsieur le président.

Je vais prendre quelques secondes pour vous remercier d'être présents, mais également pour souligner la qualité de vos présentations et de vos réponses. C'est vraiment une séance très intéressante. Le sujet en soi est fascinant, et vos interventions sont pertinentes.

Il y a plusieurs années, j'ai été frappé, comme plusieurs, par le roman *1984*, de George Orwell. Dans ce livre, on voyait le gouvernement tout-puissant devenir un *big brother* et surveiller la vie des gens. Le portrait que vous dressez de la situation nous donne l'impression que le gouvernement peut en effet être un *big brother*. Quand les conservateurs présentent un projet de loi comme le projet de loi C-30, on en a froid dans le dos, et avec raison.

Or j'ai l'impression qu'il y a une multitude de « *medium brothers* », en l'occurrence de grandes compagnies sur Internet. Ces gens arrivent à connaître nos vies, à nous surveiller, à savoir ce que nous aimons ou n'aimons pas, ce que nous achetons ou n'achetons pas, ce qui nous intéresse ou ne nous intéresse pas. Ils peuvent alors agir.

Avez-vous l'impression que les médias sociaux et Internet sont devenus un tas de *big brothers*?

● (1220)

Mme Teresa Scassa: Lorsqu'on cite le livre de George Orwell, on cite aussi souvent le film *Minority Report*, qui met en vedette Tom Cruise. Dans ce film, on voit que les annonces publicitaires changent selon la personne qui les regarde. Je crois que nous sommes en effet de plus en plus surveillés par les compagnies. Par contre, il faut noter que les renseignements recueillis par ces dernières sur nos activités, nos habitudes, l'endroit où nous nous trouvons et nos déplacements sont également accessibles au gouvernement.

Des dispositions de la Loi sur la protection des renseignements personnels et les documents électroniques, par exemple, donnent aux compagnies la possibilité de partager ces renseignements sans obtenir de consentement dans le cas d'une poursuite ou d'une enquête par les autorités. C'est de plus en plus fréquent. Mon collègue le professeur Geist l'a mentionné. Nous sommes surveillés par des compagnies dans un contexte où le gouvernement a lui aussi accès à ces renseignements. Ça vaut vraiment la peine d'être noté.

M. Alexandre Boulerice: Merci.

Quelqu'un d'autre veut-il intervenir?

[*Traduction*]

M. Michael Geist: Oui. Je veux revenir à la toute première mise en garde pour souligner à quel point ces services sont importants et précieux.

Je prends acte les propos au sujet de *big brother* et des médias sociaux, mais je tiens à souligner la valeur considérable que recèle cet outils à divers égards, que ce soit pour la communauté, l'activisme, la culture ou l'éducation, car en évoquant *big brother*, on y conférerait clairement une aura négative.

Je considère que l'argument de Mme Scassa est absolument crucial, et c'est l'une des raisons pour lesquelles j'en ai parlé dans mon exposé. Il y a 10 ans, les tenants de la protection des renseignements personnels s'inquiétaient énormément de la possibilité que des pays comme les États-Unis créent d'immenses bases de données omniscientes, qui portaient des noms comme Echelon, Carnivore ou Total Information Awareness, ou TIA. À ce que nous sachions, jamais le gouvernement n'a pu créer de telles bases de données aux États-Unis. Par contre, le secteur privé a réussi à faire quelque chose de très semblable, puisque bien des gens transmettent activement de l'information aux entreprises, qui réussissent bien souvent à en tirer une valeur réelle.

Le danger qui nous guette, c'est que les restrictions que prévoient les lois, comme la Loi sur la protection des renseignements personnels, qui pourraient limiter ce que peut faire le gouvernement avec l'information qu'il récolte, n'ont pas été établies de la même manière pour l'information recueillie par le secteur privé, puis utilisée par le gouvernement. Le gouvernement contourne ou esquive ainsi les règles qu'il s'est lui-même imposées afin de permettre à des organismes d'exécution de la loi ou à d'autres intervenants de récolter l'information auprès de tiers et d'avoir des renseignements que la loi ou d'autres dispositions lui interdisent de recueillir ou d'utiliser.

[*Français*]

M. Alexandre Boulerice: Merci; le temps file.

Je ne suis pas contre les médias sociaux. J'adore Facebook et Twitter. Ils me permettent de suivre l'actualité de façon incroyable et de partager des vidéos, de l'information et des photos que les gens prennent.

J'aimerais vous poser une question, brièvement, sur le modèle d'entreprise. Il y a quelques années, un patron de TF1, la télévision privée française, avait dit qu'il vendait à Coca-Cola du temps de cerveau humain disponible. Cela voulait dire que son travail était d'amener des téléspectateurs à regarder des publicités. C'est un peu comme quand vous achetez un journal: vous pensez que vous achetez des articles, mais vous n'achetez pas des articles, vous venez plutôt de vous vendre aux publicitaires qui annoncent dans le journal.

Dans le fond, même si on utilise et qu'on adore Facebook, Twitter et Google, il faut que les gens prennent conscience qu'ils donnent volontairement leurs informations personnelles à une compagnie qui, par la suite, fera affaire avec des industries à qui elle vendra ces informations pour être capable de modeler et cibler la publicité qui sera envoyée aux gens. Est-ce exact?

● (1225)

[*Traduction*]

M. Michael Geist: Eh bien, je crois que c'est on ne peut plus juste. À ce que nous sachions, le modèle d'affaire de ces entreprises — qui, dans bien des cas, évolue — consiste à obtenir l'information, à établir le profil social et à y ajouter de la valeur à l'intention de spécialistes du marketing ou d'autres intéressés. Il ne fait aucun doute que c'est le modèle. À mon avis, ce n'est pas mauvais en soi. Cet environnement est porteur d'une valeur considérable.

Le danger survient quand, comme je l'ai souligné plus tôt, on utilise les médias sociaux à mauvais escient ou recueille l'information à des fins que je considère souvent douteuses, et ce, à l'insu des intéressés. Ces derniers sont surveillés quand ils fournissent de l'information d'autres façons que celles qui viennent habituellement à l'esprit, comme remplir un formulaire en ligne ou télécharger des photos. En fait, ce sont les autres activités qui sont surveillées et exploitées activement, d'une manière très semblable à celle que vous avez décrite.

[*Français*]

Le président: Merci.

Malheureusement, votre temps de parole est écoulé.

Je cède maintenant la parole à M. Dreeshen, qui dispose de cinq minutes.

[*Traduction*]

M. Earl Dreeshen (Red Deer, PCC): Merci beaucoup, monsieur le président.

Je vous remercie sincèrement de témoigner aujourd'hui.

J'ai vu récemment une publicité à la télévision, dans laquelle quelqu'un peut, au moyen d'un téléphone cellulaire, capter un discours donné par un entraîneur à son équipe, s'émerveillant de pouvoir transmettre le tout par l'entremise de YouTube pour permettre à l'école de les encourager. Mais je réfléchis à ce que vous avez dit sur le mauvais usage des médias sociaux. Ces gens ne voient que le merveilleux de la chose, alors que vous regardez aussi l'autre côté de la médaille.

J'ai enseigné pendant de nombreuses années. Quand j'étais à l'université, j'ai toujours trouvé pratique de pouvoir emprunter les notes de quelqu'un quand je ne pouvais assister aux cours. Mais maintenant, il suffit de demander à quelqu'un d'enregistrer le cours et de l'envoyer ensuite à ses amis. J'ai alors commencé à m'interroger sur la pertinence du document produit par l'entraîneur et de toutes les autres utilisations, ainsi que sur les mesures de protection dont on dispose.

Qu'il existe ou non un lien avec les questions de protection des renseignements personnels dont nous traitons aujourd'hui, il faut néanmoins que les gens sachent ce qu'il en est. Les établissements doivent commencer à établir certaines règles dans les écoles afin de restreindre l'utilisation de Facebook, de téléphones cellulaires ou d'autres outils dans les salles de classe.

Voilà donc le genre de choses que j'entrevoie. Comme nous tentons d'élaborer une politique et de réfléchir sur la question, j'aimerais connaître votre point de vue à ce sujet.

Mme Valerie Steeves: Dans le cadre des projets relatifs aux jeunes Canadiens, nous nous sommes informés auprès de 10 enseignants clés. Je dispose donc de solides informations à ce sujet. Ils considèrent qu'il s'agit d'un problème de protection des renseignements personnels, car quand les murs de la classe deviennent transparents, on ne peut plus créer de lieu sûr où les enfants peuvent commettre des erreurs, explorer et apprendre efficacement. De plus, toutes sortes de problèmes surviennent quand les enfants filment secrètement ce qui se passe en classe et diffusent ensuite le tout sur Internet. Cela perturbe considérablement la dynamique.

Ces professeurs considéraient tous que la solution ne consistait pas à se débarrasser de la technologie. C'est la réaction qui nous vient en fait par réflexe: se débarrasser de ce qui nous déplaît. Or, les réseaux sociaux et les outils connexes peuvent vraiment permettre d'approfondir l'éducation des enfants, comme le corrobore un rapport sur des pratiques exemplaires vraiment formidables.

Les enseignants nous ont toutefois indiqué que le vrai problème vient du fait que les écoles empruntent la voie de l'interdiction. Si les établissements autorisent les jeunes à aller en ligne, ils les soumettent à une surveillance complète. Mais en agissant de la sorte, ils surveillent également les enseignants. Ces derniers ne peuvent donc plus tenir leur rôle d'adulte attentif, qui est là quand les enfants rencontrent des difficultés ou quand ils s'exclament « Hé, en voilà un drôle de site », auquel cas ils peuvent aller voir ce qu'il en est et informer l'enfant que c'est un site haineux.

Ainsi, en rejetant la technologie, on sonne également le glas de ces moments propices à l'enseignement, au cours desquels on peut impartir aux jeunes de véritables compétences dans le domaine numérique. Du même souffle, je ferais remarquer que c'est une question qui concerne la protection de la vie privée.

M. Michael Geist: Je considère que l'utilisation de ces outils, particulièrement à des fins éducatives, recèle un potentiel énorme. Par exemple, la présente audience n'est pas seulement regardée; j'ai jeté un coup d'oeil rapide et il y a également des gens qui gazouillent à son sujet pendant qu'ils l'écoutent ou la regardent en temps réel. La salle de classe n'est pas uniquement la salle de classe à laquelle nous avons tendance à penser, disons, à l'Université d'Ottawa. En un sens, nous sommes ici une salle de classe où d'autres personnes peuvent regarder, écouter, interagir et participer.

Alors, je crois qu'il y a d'excellentes occasions ici. Une des choses auxquelles le gouvernement devrait réfléchir, c'est sur la façon de rendre encore plus accessible l'utilisation de ce genre d'outil et de technologie pour mettre des occasions d'éducation à la portée du plus grand nombre de personnes possible.

Par exemple, le projet de loi C-11, le projet de loi sur le droit d'auteur, a fait certaines de ces choses, mais en même temps, il compte des dispositions sur l'apprentissage à distance qui exigent, comme vous le savez peut-être, que les enseignants détruisent les leçons qui sont utilisées en vertu de cette exception particulière dans un délai de 30 jours. À mes yeux, il s'agit d'une disposition très regrettable, d'une disposition qui, je pense, nous engage dans la mauvaise direction lorsque nous commençons à discuter de la façon d'utiliser ces outils dans le but de promouvoir une meilleure éducation, de meilleures occasions d'apprentissage et, franchement, de rendre l'éducation accessible à plus de gens, et non à moins de gens.

● (1230)

M. Earl Dreeshen: Madame Scassa.

Mme Teresa Scassa: Je suis d'accord. Je pense qu'il y a là un potentiel énorme du point de vue de la créativité, du dynamisme, de la possibilité de rejoindre des apprenants ayant des styles différents et des aptitudes différentes, et de la possibilité d'amener l'information et les ressources dans les classes. Il y a là un potentiel extraordinaire.

Ce que je vois, et c'est purement anecdotique en tant que parent, c'est qu'il n'y a pas beaucoup d'orientation donnée par les écoles, pas beaucoup d'information. Ma fille de 10 ans a ramené à la maison un formulaire sur l'utilisation acceptable de l'informatique qu'elle devait signer avant de pouvoir aller au laboratoire d'informatique. Sur le formulaire, on pouvait lire des choses comme: « Je m'engage à ne pas porter atteinte au droit d'auteur ». Je lui ai demandé si elle comprenait ce que veut dire l'atteinte au droit d'auteur et les activités qui constitueraient une telle atteinte. Elle n'en avait pas la moindre idée. Il y a plein d'adultes qui n'en ont pas la moindre idée. Est-ce que quelqu'un à l'école lui en avait parlé? Non.

Il n'y a tout simplement pas beaucoup de dialogue. Je pense que le rôle du gouvernement dans ces contextes, peut-être, comme cela a été dit déjà, est de favoriser l'éducation, de fournir plus d'occasions aux groupes communautaires et aux autres organismes d'exercer ces fonctions. Il y a une richesse d'occasions, mais je pense qu'il y a en même temps une pauvreté d'information et d'éducation.

[*Français*]

Le président: Merci.

Comme nous devons discuter de nos travaux un peu plus tard, je vais laisser deux minutes et demie à M. Angus et deux minutes et demie à Mme Davidson. Des questions un peu plus courtes vont nous permettre de conclure.

Monsieur Angus, vous disposez de deux minutes et demie.

[*Traduction*]

M. Charlie Angus: Merci.

C'est une discussion fascinante. Je pense certainement que nous devons toujours garder le potentiel à l'esprit. Effectivement, la participation démocratique dans les nouveaux médias a une grande valeur de transformation.

Ma préoccupation est la question du détournement d'usage, cette notion que nous entendons autour de la table qui veut que si vous signez une entente, vous donnez votre consentement. Mais vous donnez votre consentement à un élément d'information précis que vous partagez et pourtant, cette information est ensuite partagée encore et encore dans cette vaste mine de données. C'est une question de droit à la vie privée qui doit être précisée lorsque vous vous inscrivez dans quelque chose.

Ma fille, qui est en 9e année, m'a envoyé un courriel l'autre jour pour me dire qu'on ne lui permettait pas d'accéder à son compte Gmail à moins qu'elle donne son numéro de téléphone cellulaire à Google. J'ai trouvé cela très étrange. Je l'ai appelée pour lui demander ce qui était arrivé. Elle m'a répondu qu'elle ne pouvait pas accéder à son compte Gmail à moins de donner son numéro de téléphone cellulaire à Google.

Le jour suivant, mon compte Gmail est apparu à l'écran et on me demandait d'inscrire, s'il vous plaît, mon numéro de téléphone cellulaire pour une plus grande sécurité. Je ne voulais pas donner mon numéro à ces gens. Ma fille de 9e année est plus futée que moi et ne leur a pas donné le sien. Vous deviez regarder tout en bas de la page pour trouver une ligne en tous petits caractères qui disait: « Cliquez ici si vous ne voulez pas le faire ».

Lorsque vous regardez cela, ces gens demandaient à ma fille de 14 ans de leur donner son numéro de téléphone cellulaire. Maintenant, Google est une entreprise citoyenne exemplaire, mais ma fille ne s'est pas inscrite à Gmail pour lui donner de l'information sur son cellulaire.

Je suppose que dans cette question de détournement d'usage, je me demande quel est notre rôle pour dire, très bien, un instant; cela dépasse les bornes. Allez-vous utiliser ce numéro de cellulaire d'une adolescente strictement pour sa sécurité personnelle ou est-ce que ce numéro sera ajouté à cette vaste mine de données à laquelle quelqu'un d'autre aura accès.

Je pense que ce sont là les questions que nous devons poser à titre de législateurs.

Mme Valerie Steeves: Peut-être puis-je ajouter une autre brève observation.

Si vous regardez la question du vol d'identité, typiquement, la solution est toujours: « Donnez-moi plus d'information à votre sujet de manière que je puisse m'assurer que c'est vous », ce qui ne fait que créer davantage de fuites, ce qui ne fait qu'accroître le risque que l'information circule et qu'elle soit utilisée contre vous.

Alors, appeler cela une mesure de « sécurité » est un peu étrange.

Mme Teresa Scassa: Pour revenir à un point qui a été soulevé plus tôt, la notion de transparence est d'une importance capitale, parce que les gens ne sont pas nécessairement conscients que l'élément d'information pour lequel ils ont donné leur consentement dans un contexte — ou pour lequel ils ont donné un certain consentement, sans avoir peut-être été conscients de l'ampleur de ce consentement… Ils peuvent ne pas avoir pris conscience de la nature de l'entente entre eux-mêmes et l'entreprise offrant des services gratuits. Beaucoup de gens ignorent que Gmail fait l'objet d'un balayage pour extraire les renseignements personnels et que cela fait partie de l'entente signée avec Gmail. Alors, il y a un manque de transparence de ce côté.

Il y a également un manque de transparence de l'autre côté, lorsque vous allez sur un site Web. Mme Steeves a décrit un certain nombre de contextes dans lesquels on vous présente des publicités lorsque vous allez lire le journal, allez sur MSN ou peu importe où. Je pense qu'il y a un manque de transparence. Les gens ne sont pas nécessairement conscients du fait que ce qu'ils voient est différent de ce que d'autres personnes voient, et qu'il y a une raison pour cela.

J'ignore si cela est en partie une question d'établir une norme. Nous avons également parlé de l'établissement de limites, de ne pas simplement permettre que tout se fasse par le biais du modèle du consentement, mais, en fait, de fixer certaines normes ou limites, ce qui, à mon avis, est une chose positive.

Ensuite, il y a la dimension de la transparence croissante et si cela consiste en une plus grande conscientisation du public ou en une obligation imposée aux entreprises d'en faire davantage pour être plus transparentes.

● (1235)

[*Français*]

Le président: Il reste 30 secondes à M. Geist pour répondre brièvement à la question.

[*Traduction*]

M. Michael Geist: Je noterais simplement qu'il y a des entreprises qui s'occupent de la question dont on nous parle, cette notion qu'ils pensent que vous êtes quelqu'un, mais que, peut-être, vous n'êtes pas cette personne. Par exemple, même Google vous donne cette possibilité, et c'est très frappant lorsque vous le faites. Google possède une section où elle vous dira qui elle pense que vous êtes et ce que vous aimez à partir de toute l'information qu'elle a pu recueillir.

Maintenant, vous pouvez lui dire de cesser de le faire si vous le désirez. Vous pouvez également lui dire qu'elle se trompe et lui dire qui vous êtes vraiment, parce que vous voulez voir des choses qui reflètent mieux vos intérêts. Certaines personnes disent qu'elles ne veulent pas dire à ces entreprises qui elles sont ou quels sont leurs intérêts. D'autres personnes disent qu'elles préfèrent voir ce genre de choses.

Le point que je veux soulever, c'est qu'il y a des entreprises qui pensent à ces questions. Si vous pouvez obtenir le bon cadre de travail avec les bons incitatifs du point de vue de la réglementation, je pense qu'il y a certaines bonnes occasions ici.

[*Français*]

Le président: Merci.

La dernière intervention revient à Mme Davidson, qui dispose d'environ deux minutes et demie.

[*Traduction*]

Mme Patricia Davidson (Sarnia—Lambton, PCC): Merci beaucoup, monsieur le président.

Ma question s'adresse à Mme Steeves.

J'étais certainement intéressée par la recherche que vous avez effectuée sur la vie privée des enfants. J'ai deux ou trois questions. Je vais les poser et ensuite, vous laisser y répondre si vous le pouvez.

Premièrement, avons-nous accès à cette étude? Quel âge avaient les enfants qui ont fait l'objet de votre recherche? Comment avez-vous défini les renseignements « personnels » ou « privés » lorsque vous parlez à ces enfants?

Nous avons connu une incidence très élevée de suicides chez les jeunes gens dans ma circonscription. Cette semaine, j'ai parlé à un parent préoccupé et affolé dont la fille de 14 ans a menacé de se suicider. Elle ne s'est pas suicidée, Dieu merci, mais les choses en sont venues à un point où le parent était fermement convaincu que ce sont les médias sociaux qui avaient fait pencher la balance et avaient constitué la pire menace pour cette enfant. Cela concernait la divulgation de renseignements qu'elle estimait personnels et qui circulaient abondamment dans la communauté de l'école.

Pourriez-vous faire des observations sur ces questions, s'il vous plaît?

Mme Valerie Steeves: L'étude a été menée auprès d'enfants de 11 à 17 ans, et de parents ayant des enfants dans cette fourchette d'âge. On peut consulter l'étude en ligne, et c'est avec plaisir que je la mettrai à la disposition du comité. Nous avons également recueilli beaucoup de données sur la cyberintimidation, ce à quoi vous faites allusion; le problème est que les gens peuvent dire des choses dans ce contexte et que les enfants peuvent mal les interpréter et perdre le contrôle.

En réalité, nos données laissent entendre le contraire. Selon les enfants à qui nous avons parlé, l'intimidation en ligne laisse une trace écrite et est donc plus facile à affronter que l'intimidation dans la vie réelle. On peut la montrer et dire: « regarde, elle a dit ça », alors on peut s'adresser à des adultes et obtenir de l'aide. Ils savent bien que les enfants sont plus susceptibles de dire des choses plus offensantes parce que ce n'est pas en personne. Ils nous ont dit: « en fait, c'est facile parce qu'on peut les confronter en personne; sinon, on peut alors s'adresser à un parent. C'est à ce moment-là qu'il vous faut l'aide de vos parents ».

Il existe peu de données empiriques qui indiquent que cette forme d'intimidation aggraverait réellement les tendances suicidaires. Des données prouvent le contraire, qu'il est en réalité plus facile d'y faire face.

Ce que les enfants nous ont clairement affirmé, et vous vous en apercevrez si vous lisez le rapport, c'est que leurs écoles répondent à l'intimidation par des politiques de tolérance zéro et par la surveillance totale. Autrement dit, ils ne peuvent rien dire à l'école, rien dire à leur professeur, même s'ils lui font confiance, parce qu'ils savent que le directeur sera appelé, que la police sera appelée et qu'ils ne contrôleront plus la situation.

À beaucoup d'égards, nous réagissons trop fortement à un problème donné et nous ne donnons pas aux enfants le soutien dont ils ont besoin, précisément parce que nous essayons de les protéger.

[*Français*]

Le président: Merci.

Cela conclut vos témoignages. Je vous remercie d'avoir été ici aujourd'hui. J'espère qu'on pourra se revoir. Je suis sûr que vos témoignages vont aider les membres du comité dans leurs délibérations.

On va suspendre la réunion pour quelques minutes.

Avant de terminer, en ce qui concerne les deux documents que Mme Steeves doit transmettre au comité, il suffit d'envoyer le lien ou les documents au greffier.

● (1240)

[*Traduction*]

Mme Valerie Steeves: Oui.

[*Français*]

Le président: On va s'assurer que tous les membres du comité pourront y avoir accès le plus rapidement possible.

Sur ce, on suspend la séance pendant quelques minutes et on passera ensuite aux travaux du comité.

● (1240)

(Pause)

● (1240)

Le président: Nous reprenons la séance.

Avant de commencer, je tiens à mentionner aux membres du comité que la commissaire à l'information a déposé ses cartes de fiches de rendement, ses *report cards*, comme on les appelle au comité. À titre d'information, si vous voulez les voir, elles sont disponibles.

Monsieur Del Mastro, voulez-vous prendre la parole avant qu'on commence?

[*Traduction*]

M. Dean Del Mastro: Monsieur le président, puisque nous passons à présent aux travaux du comité, je propose de passer à huis clos.

[*Français*]

Le président: On ne peut malheureusement pas débattre de cette motion.

M. Alexandre Boulerice: Je demande la tenue d'un vote par appel nominal.

Le président: Dans ce cas, je vais laisser le greffier procéder au vote.

(La motion est adoptée par 6 voix contre 4. [Voir le *Procès-verbal*])

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