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 046 • 1re SESSION • 41e LÉGISLATURE

TÉMOIGNAGES

Le mardi 19 juin 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 mardi 19 juin 2012

● (1100)

[*Français*]

Le président (M. Pierre-Luc Dusseault (Sherbrooke, NPD)): Comme il est 11 heures, nous allons commencer la réunion immédiatement.

Je remercie M. Kardash, de Heenan Blaikie, et Mme Grimes, de l'Université de Toronto, d'être parmi nous aujourd'hui. Nous attendons deux autres témoins qui devaient être ici à 11 heures. Selon nos informations, ils sont en route.

Nous allons commencer par les présentations, qui seront d'une durée de 10 minutes. Il y aura ensuite des périodes de questions et réponses.

Je vais donc sans plus tarder céder la parole à Mme Grimes.

[*Traduction*]

Mme Sara Grimes (professeure adjointe, Faculté de l'information, Université de Toronto): Je vous remercie de me donner l'occasion de m'adresser à vous aujourd'hui.

Au cours des dernières années, j'ai axé ma recherche sur certains des sites de médias sociaux les plus populaires auprès des enfants, des cybercommunautés comme Neopets aux environnements virtuels comme Club Penguin. Ces sites ne ressemblent pas vraiment à Facebook, mais ils permettent néanmoins le même type d'interactions sociales et d'activités qui sont propres aux médias sociaux.

Les questions relatives à la vie privée revêtent une grande importance au sein de ces environnements. Des études démontrent que dès les débuts du Web, le droit à la vie privée des enfants a été bafoué à des fins commerciales dans certains forums sociaux en ligne. C'est beaucoup plus fréquent que la plupart des autres risques associés à l'utilisation d'Internet par les enfants. Dans d'autres pays, cela a mené directement à l'adoption de mesures législatives sur la protection de la vie privée des enfants, dont l'exemple le plus frappant est la Children's Online Privacy Protection Act, ou COPPA, aux États-Unis, qui a été élaborée en réponse à la pratique de plus en plus fréquente, à l'époque, de demander les noms et adresses des enfants afin de les solliciter directement.

Aujourd'hui, le type de données recueillies auprès des enfants et l'usage qu'on en fait se sont accrus considérablement. L'article qui vous a été distribué avant ma comparution décrit en détail ce changement et explique les tendances de l'industrie relativement à l'exploration de données, au cours de laquelle on se sert des conversations, des comportements et des idées des enfants pour alimenter les études de marché et le développement de produits.

Dans le cadre de mes travaux dans ce domaine, j'ai constaté que dans les médias sociaux, lorsqu'on tient compte des enfants, le respect de leurs droits ne passe souvent qu'après les notions de risque définies de façon restrictive. On considère encore beaucoup les enfants comme des victimes potentielles ou, à l'inverse, des criminels potentiels dans l'environnement virtuel. Ainsi, on met l'accent sur la protection des enfants contre les étrangers, contre les autres enfants et contre eux-mêmes, au lieu de les soutenir et de les aider en tant que citoyens.

Cette tendance a eu des effets importants sur la manière dont les entreprises de médias sociaux traitent les utilisateurs mineurs. La réaction la plus fréquente a été tout simplement d'interdire aux enfants de moins de 13 ans d'utiliser les sites de médias sociaux. C'est la stratégie qui a été utilisée jusqu'à tout récemment par Facebook, et elle demeure fréquente également dans les autres médias sociaux populaires. Même si des enfants peuvent contourner et contournent souvent ces interdictions — en mentant au sujet de leur âge, par exemple —, une limite d'âge officielle a tout de même des effets importants sur la façon dont les enfants utilisent les médias sociaux et l'endroit où ils le font. Cela permet également aux médias sociaux de se soustraire un peu à l'examen public et à la surveillance réglementaire dont peuvent faire l'objet les sites qui acceptent les enfants ou les invitent à participer.

Bien que dans certains cas, les restrictions liées à l'âge peuvent très bien être appropriées — elles le seraient pour bien des sites —, dans d'autres, l'approche qui consiste à ne pas accepter les enfants vise davantage à éviter les risques et les complications liés aux enfants qu'à les protéger du contenu ou des activités du site. Cela signifie que l'on interdit fréquemment aux jeunes enfants de participer pleinement à la culture en ligne et de profiter des nombreux avantages et des nombreuses possibilités qu'offrent les médias sociaux, uniquement parce que l'on considère que c'est trop de travail, trop coûteux ou simplement trop risqué de le leur permettre.

Il y a une autre réaction de plus en plus fréquente, et c'est la création de médias sociaux rigoureusement contrôlés destinés aux enfants, que l'on trouve dans les sites de réseautage social, les environnements virtuels et les cybercommunautés destinés habituellement aux enfants de moins de 13 ans. Dans le cadre de ma recherche, j'ai constaté que bien souvent, en mettant l'accent sur les risques, on met la protection de la vie privée au premier plan. Les questions liées à la protection de la vie privée intégrées à l'étape de la conception sont assez évidentes. Elles apparaissent dans les documents juridiques comme les politiques de confidentialité relatives à l'utilisation et elles sont présentées dans la promotion des sites eux-mêmes.

Toutefois, de nombreux aspects ont grandement besoin d'être améliorés. Comme on l'a mentionné, il est prouvé que les interactions en ligne des enfants sont surveillées et explorées, la plupart du temps sans que les enfants, ni les parents ou les tuteurs, en soient informés ni y aient consenti. Même si les enfants doivent régulièrement accepter ce type d'activités dans les politiques sur la confidentialité et les conditions d'utilisation pour pouvoir participer, même sur les sites destinés aux jeunes enfants, ces documents sont longs et extrêmement complexes. Ils décrivent une grande variété d'activités de collecte de données et comprennent de nombreux termes qui sont inappropriés et qui ne peuvent pas même être utilisés pour demander le consentement des enfants.

Cela soulève d'importantes questions au sujet du consentement éclairé, un problème particulièrement préoccupant, étant donné que parmi les utilisateurs figurent de jeunes enfants dont le niveau d'alphabétisation et les capacités de comprendre les rapports juridiques complexes varient énormément. Idéalement, il faudrait fournir une version de ces documents qui serait adaptée aux enfants pour s'assurer que les enfants et leurs parents savent précisément ce à quoi ils consentent. Même s'il existe d'excellents exemples de cette pratique, il y a très peu de sites destinés aux enfants qui se donnent la peine de le faire. Lorsqu'ils le font, les versions adaptées aux enfants sont rarement complètes; la plupart n'expliquent pas en détail les raisons de la collecte des données de l'utilisateur ou ne décrivent que les éléments qui présentent l'entreprise de médias sociaux sous un jour favorable.

● (1105)

Il existe aussi une tendance de plus en plus répandue qui consiste à affirmer faussement que les renseignements personnels des enfants sont une question de sécurité en ligne. Mais ne vous méprenez pas. Concrètement, il est très avantageux pour la sécurité des enfants et leur droit de profiter des médias sociaux d'examiner de façon approfondie dans quelle mesure les règles et les caractéristiques de conception visant à protéger les droits à la vie privée des enfants pourraient aussi offrir une protection contre les prédateurs et les intimidateurs en ligne. Mais jusqu'ici, dans bien des cas, on s'est servi de cette double fonction principalement pour masquer les pratiques commerciales sous-jacentes que les politiques relatives à la protection des renseignements personnels visent à éliminer. En présentant la protection des renseignements personnels des enfants comme étant principalement une question de sécurité en ligne — que l'on définit, dans ces cas, comme une protection contre les autres utilisateurs — on occulte les menaces plus courantes et moins importantes à la protection des renseignements personnels des enfants, comme la surveillance par les entreprises et les études de marché qui portent atteinte à la vie privée.

Il y a une tendance émergente connexe qui consiste à commercialiser les caractéristiques de sécurité elles-mêmes, comme je l'ai découvert dans une étude récente sur les mondes virtuels pour enfants. Certains mondes virtuels ont une version de « clavardage sécuritaire », dans laquelle le clavardage entre utilisateurs se limite à sélectionner des phrases préconstruites à partir d'un menu déroulant. Dans un cas, la version « clavardage sécuritaire » limitait les options des enfants à 323 phrases, dont 45 servaient à la publicité croisée et 30 présentaient des annonces de tiers. Comme vous l'aurez deviné, aucune de ces phrases n'était négative. Les enfants pouvaient indiquer comment ils aimaient la marque, mais ils ne pouvaient pas dire quoi que ce soit de négatif à son sujet.

Cela peut avoir, entre autres, des effets négatifs sur les droits des enfants. Ces exemples indiquent qu'un malheureux compromis a lieu, puisque les stratégies limitées de sécurité et de protection des renseignements personnels des enfants peuvent restreindre indûment leurs autres droits, comme le droit à la liberté d'expression ou le droit de participer librement à la vie culturelle.

Il est important de souligner que j'ai décrit ici des tendances générales, dont la plupart sont utilisées dans les sites commerciaux de médias sociaux considérés comme les plus populaires auprès des enfants. Ce ne sont pas toutes les entreprises qui utilisent ces pratiques. En fait, il y a des entreprises canadiennes qui ont adopté des stratégies de remplacement assez brillantes afin de créer un équilibre entre la protection des renseignements personnels, la sécurité, l'expression personnelle et la participation culturelle des enfants. Il est possible de faire preuve ici d'un véritable leadership, mais actuellement, le soutien nécessaire, sur le plan réglementaire et gouvernemental, n'est pas suffisant pour que ces approches individuelles, éthiques, axées sur les droits et d'ampleur limitée deviennent une pratique répandue dans l'industrie.

Je vais prendre le temps qu'il me reste pour vous parler de quatre priorités clés ou recommandations.

Premièrement, il y a un besoin évident et grandissant de mettre en place une réglementation adaptée aux enfants en ce qui concerne la collecte, la gestion et l'utilisation des données relatives aux enfants. Cependant, il nous faudra éviter de répéter les erreurs qui ont nui à certaines des tentatives antérieures, comme la COPPA, aux États-Unis. Cette loi a eu comme conséquence de priver les enfants de l'accès à certains espaces sociaux très importants ou de les inciter à mentir systématiquement au sujet de leur âge. Il nous faudra également étendre cette réglementation de façon à mieux refléter les pratiques actuelles et futures en matière de collecte de données en ligne.

Deuxièmement, il nous faut préciser beaucoup plus clairement l'éthique relative au consentement éclairé lorsqu'il s'agit d'enfants de divers groupes d'âge.

Troisièmement, nous devons atteindre un meilleur équilibre entre les droits de protection des renseignements personnels des enfants et les autres droits, comme la liberté d'expression et le droit de participer à la vie culturelle, dans nos discussions sur ces questions comme dans la réglementation, qu'elle soit nouvelle ou modifiée.

Finalement, nous devons exercer un véritable leadership et renforcer l'application de ces règles adaptées aux enfants, notamment la reconnaissance et le soutien des stratégies novatrices, éthiques et axées sur les droits que certaines petites entreprises indépendantes canadiennes de médias sociaux s'emploient déjà à développer.

Je me ferai un plaisir de discuter plus en détail de ces enjeux durant la période des questions.

Merci.

● (1110)

[*Français*]

Le président: Merci beaucoup.

Je vais maintenant céder la parole à M. Israel.

Vous disposez de 10 minutes.

[*Traduction*]

M. Tamir Israel (avocat-conseil à l'interne, Clinique d'intérêt public et de politique d'Internet du Canada): Bonjour.

Je m'appelle Tamir Israel et je suis avocat-conseil à l'interne à la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko, ou CIPPIC. La CIPPIC vous remercie de lui donner l'occasion de vous présenter son point de vue sur les incidences des médias sociaux sur la vie privée.

La CIPPIC est une clinique juridique située au Centre de recherche en droit, technologie et société de l'Université d'Ottawa. Nous défendons l'intérêt public sur des questions se situant à l'intersection du droit et de la technologie.

Depuis sa fondation, la CIPPIC joue un rôle actif dans les débats politiques et juridiques relatifs à la protection de la vie privée en ligne, tant à l'échelle nationale qu'internationale. Notre clinique a déposé une plainte qui a mené à la première enquête complète sur les pratiques en matière de vie privée des réseaux sociaux internationaux.

[*Français*]

Le président: Un instant, monsieur Israel. Pourriez-vous lire un peu moins vite, s'il vous plaît, de façon à ce que les interprètes puissent bien faire leur travail?

[*Traduction*]

M. Tamir Israel: Je vais parler un peu plus lentement.

On ne saurait sous-estimer l'importance grandissante et les avantages des médias sociaux pour les Canadiens. Ils ont une portée considérable et imprègnent tous les aspects de notre vie personnelle, sociale et politique. La croissance innovatrice et commerciale de tels réseaux ne devrait pas être restreinte indûment. En même temps, les Canadiens ne devraient pas avoir à choisir entre leur droit à la vie privée et leur droit de participer à ce nouvel environnement interactif.

La LPRPDE, qui constitue l'épine dorsale de la réglementation sur la protection des renseignements personnels au Canada, fournit un ensemble de principes souples qui pourvoient aux besoins légitimes des entreprises tout en offrant des mesures de protection pour les renseignements personnels des utilisateurs. Bien que la LPRPDE ait très bien résisté à l'épreuve du temps, la protection des renseignements personnels a considérablement évolué depuis son adoption, et une décennie d'expérience a mis en lumière un certain nombre de lacunes qui doivent être corrigées pour que la loi puisse continuer à atteindre ses objectifs.

Je vais vous parler brièvement des changements à la protection de la vie privée, puis j'aborderai quatre points qui requièrent, selon moi, une attention immédiate.

Dans un récent témoignage devant le comité, Mme Valerie Steeves a signalé que des études soulignent un manque de confiance envers les entreprises en ligne. Un sondage réalisé pour Ressources naturelles Canada à la fin de 2009 a révélé que le niveau de confiance des répondants à l'égard de divers types d'organisations en ce qui concerne la sécurité de leurs renseignements personnels varie de modéré à faible. Celles qui inspirent le moins confiance sont les petites entreprises privées et les sites de réseautage social.

De même, l'étude a révélé que la capacité à contrôler l'environnement dans lequel les renseignements sont partagés permettait d'augmenter le niveau de confiance. Une autre étude effectuée par des chercheurs d'Annenberg et de Berkeley indique que 67 p. 100 des Américains étaient d'accord ou fortement d'accord pour dire que les utilisateurs ont perdu tout contrôle sur la manière dont les renseignements personnels sont recueillis et utilisés par les entreprises.

Ce qui alimente ce sentiment de perte de maîtrise est un écosystème de plus en plus complexe dans lequel la portée et la nature des données recueillies augmentent de jour en jour, tandis que le raffinement de la collecte des renseignements et des mécanismes d'analyse évolue au même rythme. Bien que Google et Facebook soient au premier plan dans les débats sur ces questions, beaucoup d'autres entreprises sont en cause. Il semble qu'Acxiom, un courtier en données de l'Arkansas, ait recueilli en moyenne 1 500 points de données sur chacun de ses 500 millions de profils d'utilisateurs actifs.

Il y a très peu de ces utilisateurs qui ont entendu parler d'Acxiom, et il y en a encore moins qui ont interagi directement avec l'entreprise. Or, les profils, que vendent les courtiers en données comme Acxiom, contiennent leurs habitudes de navigation; leurs discussions avec leurs amis et les membres de leur famille sur Facebook; leurs renseignements médicaux et financiers sensibles; leur ethnie, leur religion et leur allégeance politique; et même les endroits réels qu'ils ont visités. Toutes ces données sont recueillies, analysées et transformées en un schéma élaboré de classification socio-économique, sur lequel les clients d'Acxiom se fondent pour prendre des décisions.

La complexité même de l'écosystème qui alimente les bases de données comme celle d'Acxiom anéantit toute tentative de faire quoi que ce soit qui respecterait une politique sur la protection des renseignements personnels. Un certain nombre de pays cherchent des façons de répondre à la nécessité d'une plus grande transparence et d'un plus grand choix. Je vais aborder brièvement quatre éléments qui, je crois, concernent précisément la LPRPDE. Je soulignerai également que la nature des données recueillies dans cet écosystème est de plus en plus sensible. De nouvelles capacités visent à inclure l'emplacement en temps réel et même l'état émotif dans les catégories de renseignements disponibles en vue du ciblage. Je vais aborder quatre changements sur lesquels nous devrions mettre l'accent. Le premier est la transparence.

Une plus grande transparence est nécessaire. À cette fin, la Federal Trade Commission des États-Unis a déclaré récemment qu'elle inciterait les courtiers de données à offrir des mécanismes électroniques centralisés qui permettront aux utilisateurs de savoir quels courtiers de données ont recueilli leurs renseignements. Cela peut servir de fondement à l'exercice d'autres droits des utilisateurs.

On peut informer les utilisateurs dans de nombreux contextes en intégrant davantage la notification dans le service même. Non seulement cela permet davantage de souplesse et de nuance, mais cela rappelle également aux utilisateurs l'importance de la protection des renseignements personnels dans le contexte des décisions qu'ils prennent dans ce domaine. De plus, les éléments des politiques de protection de la vie privée peuvent être normalisés, mais il faut prendre garde à ne pas simplifier exagérément les pratiques relatives aux données, qui sont en réalité complexes. Les dangers liés à la simplification exagérée sont que les organisations commenceront à compter sur le consentement général et le consentement catégorique, qui sont simples, mais qui ne donnent pas aux consommateurs ni aux groupes de défense les détails dont ils ont besoin pour évaluer adéquatement leurs pratiques.

● (1115)

Un autre point que j'aimerais aborder, c'est la protection implicite de la vie privée ou son pendant, la protection de la vie privée moyennant certains efforts.

La transparence, à elle seule, ne suffit pas pour protéger la vie privée en cette époque où tout est très étroitement lié. Dans le cadre d'une récente consultation sur la protection de la vie privée en ligne, on a fait remarquer que de nombreux services en ligne sont publics par défaut et privés moyennant certains efforts. Au moment de s'inscrire pour la première fois, les nouveaux utilisateurs savent rarement comment configurer l'ensemble complexe de services de contrôle de la confidentialité, qui sont d'ailleurs souvent conflictuels. Les paramètres changent constamment, à mesure que de nouvelles fonctions viennent remplacer les anciennes ou que d'autres attributs viennent se greffer aux services existants. Pour maintenir un niveau constant de confidentialité, il faut donc déployer sans cesse des efforts.

À cela s'ajoute la tendance des sites de réseautage social à faire, de temps à autre, des virages profonds dans la constitution et la nature de leurs services. Ces changements sont souvent imposés aux utilisateurs invétérés, et c'est « à prendre ou à laisser ». D'autres fois, les sites utilisent des paramètres présélectionnés par défaut afin d'amener les utilisateurs à choisir des options qui sont très différentes du service auquel ils sont habitués.

Comme d'autres spécialistes vous l'ont dit, il faut faire attention aux paramètres par défaut, et c'est là que le bât blesse. Des mesures de protection plus rigoureuses s'imposent pour s'assurer que les nouveaux services et attributs comportent des paramètres par défaut qui favorisent la protection de la vie privée et qui tiennent compte des attentes des utilisateurs et de la nature délicate des données en question, au lieu de s'en tenir aux configurations qui conviennent le mieux au modèle d'affaires du fournisseur de services.

Aux termes de la LPRPDE, la formule de consentement devrait toujours être adaptée aux attentes des utilisateurs et à la nature délicate des données pouvant être touchées. Toutefois, pour que ce concept soit fermement implanté dans la conception des services, on devrait intégrer à la LPRPDE le principe de la protection implicite de la vie privée.

Par ailleurs, j'aimerais vous parler brièvement de l'application de la loi et du processus.

Plusieurs témoins qui ont comparu devant le comité ont parlé de l'importance de s'assurer que le Commissariat à la protection de la vie privée peut appliquer ses pouvoirs. Il est essentiel de donner du mordant à la LPRPDE et ce, pour plusieurs raisons. D'abord, cela encourage la conformité. À l'heure actuelle, il y a très peu de pénalités pour la non-conformité. Dans la plupart des cas, la pénalité maximale à laquelle une organisation peut s'attendre, c'est la menace de subir une humiliation publique pour cause de non-conformité. Deuxièmement, la mise en place de ces pouvoirs aidera le Commissariat à la protection de la vie privée dans ses interactions avec les grandes organisations multinationales et dans l'acquittement de son mandat qui consiste à protéger la vie privée des Canadiens.

Outre l'ajout de pénalités, on devrait envisager de modifier les procédures du commissariat en ce qui a trait au cadre d'enquête et de surveillance de la conformité. Dans le contexte du réseautage social, la conformité aux recommandations du commissariat risque d'être un chemin long et compliqué, qui nécessitera des changements à la conception des systèmes. Toutefois, aux termes de la LPRPDE, le commissariat dispose d'un délai de 45 jours, après avoir rendu publiques ses conclusions officielles, pour exercer son mandat légal par rapport à une plainte particulière. Le mécanisme n'a pas la souplesse nécessaire pour permettre d'appliquer, en bonne et due forme, les recommandations de la Commissaire à la protection de la vie privée.

Enfin, je vais parler brièvement des exigences en matière de notification des atteintes à la protection des données.

Le Canada a grand besoin d'une obligation de notification des atteintes à la protection des données. Une telle obligation encouragera l'établissement de mesures de protection techniques plus musclées et donnera aux utilisateurs la possibilité de réparer le tort qui leur est fait, comme le vol d'identité et l'humiliation potentielle à la suite d'une atteinte à leurs données.

Le projet de loi C-12, qui en est à l'étape de la première lecture, prévoit un cadre raisonnable pour la notification des atteintes à la protection des données, sous réserve de quelques ajustements et d'un engagement à imposer des pénalités pour la non-conformité, afin d'en assurer l'efficacité.

Je serai heureux d'approfondir certains de ces points. Sachez que la CIPPIC prévoit envoyer au comité un mémoire plus détaillé à une date ultérieure.

Merci beaucoup de votre temps et de votre attention.

● (1120)

[*Français*]

Le président: Je vous remercie de nous avoir livré votre présentation.

Nous allons maintenant passer à M. Kardash, pour 10 minutes également.

[*Traduction*]

M. Adam Kardash (directeur général, Access Privacy, Heenan, Blaikie): Bonjour, monsieur le président et mesdames et messieurs les membres du comité. Merci de me donner l'occasion de m'adresser à vous aujourd'hui.

Je m'appelle Adam Kardash. Je suis un associé du cabinet juridique national Heenan Blaikie, où je préside le groupe national sur la protection des renseignements personnels et de la gestion de l'information. Je suis également directeur général et chef d'Access-Privacy, un service de consultation et d'information de Heenan Blaikie qui vise le respect des renseignements personnels.

Je comparais aujourd'hui devant le comité à titre personnel pour représenter mon propre point de vue. Toutefois, sachez que mes opinions reposent sur mon expérience chez Heenan Blaikie et AccessPrivacy.

Au cours des 10 dernières années, j'ai concentré ma pratique presque exclusivement sur les questions liées à la protection des renseignements personnels et à la gestion de l'information à l'intention d'organisations du secteur privé. J'examine régulièrement les conséquences des nouvelles technologies et plateformes dans le contexte des lois en matière de protection de la vie privée.

Dans mes observations préliminaires, je ferai quelques commentaires pour faire ressortir un message bien précis, à savoir que notre loi fédérale sur la protection des renseignements personnels dans le secteur privé, soit la Loi sur la protection des renseignements personnels et les documents électroniques ou la LPRPDE, fonctionne très bien. Depuis son entrée en vigueur en 2001, et malgré les diverses critiques soulevées au départ par une foule d'intervenants dans le domaine canadien de la protection des renseignements personnels, cette loi a tout de même résisté à l'épreuve du temps. Selon moi, le point fort de la LPRPDE a été et continue d'être le fait qu'elle nous permet de relever les défis posés par les nouvelles technologies relativement à la protection de la vie privée.

La loi établit un ensemble complet d'exigences qui régissent la façon dont une organisation recueille, utilise, communique, met en mémoire et gère des renseignements personnels. Une des raisons pour lesquelles la loi demeure efficace aujourd'hui, c'est parce que son libellé est neutre sur le plan technologique. En gros, les règles de base de la LPRPDE sont énoncées dans un langage simple sous forme de principes généraux. Elles peuvent donc s'appliquer à tout nouveau système, technologie ou application qui met en jeu le traitement de renseignements personnels, et cela comprend aussi les plateformes des médias sociaux.

La LPRPDE ne vise aucun type de technologie en particulier, et c'est justement pourquoi elle parvient si bien à régler de soi-disant nouveaux problèmes en matière de protection de la vie privée attribuables aux progrès technologiques. À cet égard, il est important que le libellé de la LPRPDE demeure neutre sur le plan technologique. En raison du rythme de plus en plus effréné des innovations technologiques, toute mesure législative qui se concentre sur une technologie ou une plateforme particulière, comme les médias sociaux, sera obsolète et dépassée, à peine entrée en vigueur.

D'après mon expérience, la façon la plus efficace de régler des questions basées sur la technologie, qu'il s'agisse de la protection de la vie privée ou d'autres enjeux, c'est de recourir à des cadres d'autoréglementation en parallèle avec le régime législatif. Comparativement aux lois ou aux règlements, les cadres d'autoréglementation sont beaucoup plus faciles à élaborer, à mettre en oeuvre, à modifier par adjonction ou à réviser en fonction de l'évolution constante des technologies.

D'ailleurs, aux termes de la LPRPDE, un cadre d'autoréglementation élaboré au moyen d'un processus de consultation valable aurait une valeur juridique. Les cadres d'autoréglementation établissent des normes industrielles et, si celles-ci sont bien conçues, elles permettent d'éclairer la définition du critère fondamental de la LPRPDE, soit celui de la personne raisonnable. Cette définition se trouve au paragraphe 5(3) de la loi, en vertu duquel une organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

Dans le cadre de ma pratique, lorsque je conseille mes clients, je n'invoque pas la LPRPDE comme un simple ensemble de règles juridiques. La loi établit plutôt un cadre utile qui permet aux organisations d'aborder de façon proactive les préoccupations liées à la protection de la vie privée, histoire de trouver le juste milieu entre la protection de la vie privée et la nécessité de recueillir, d'utiliser et de communiquer des renseignements personnels dans le cadre d'activités commerciales légitimes. Les règles de la LPRPDE sont dynamiques, en ce sens qu'elles s'appliquent au cycle de vie entier des données, de la collecte ou de la création jusqu'à la destruction éventuelle des renseignements personnels détenus par une organisation.

Toutes ces règles relèvent de l'attribut principal de la LPRPDE: le principe de la responsabilité. Bien qu'il soit formulé en termes simples, le principe de la responsabilité est une exigence très puissante, en vertu de laquelle les organisations sont responsables des renseignements personnels qu'elle ont en leur possession ou sous leur garde.

Des organismes partout dans le monde, qu'il s'agisse d'organismes étrangers chargés de la protection des données, d'organismes gouvernementaux étrangers ou de groupes de réflexion internationaux sur la protection de la vie privée, considèrent désormais le principe de responsabilité prévu dans la LPRPDE comme un modèle législatif éclairé pour la protection des renseignements personnels. Si le cadre de la LPRPDE a la cote auprès de ces forums internationaux, c'est surtout à cause de son modèle de responsabilité qui permet, dit-on, de bien régler les problèmes en matière de protection de la vie privée susceptibles de surgir dans le monde virtuel ou, encore, dans le contexte technologique.

● (1125)

Comme le démontrent clairement un certain nombre de lettres de conclusions publiées par le Commissariat à la protection de la vie privée du Canada, le cadre actuel de la LPRPDE permet au commissariat d'examiner et de résoudre de façon efficace de nouvelles questions en matière de protection de la vie privée soulevées par les nouvelles technologies. Plusieurs de ces lettres portent aussi sur le contexte des médias sociaux.

Une des caractéristiques principales et, selon moi, essentielles de la LPRPDE est le modèle d'ombudsman qui est intégré à la loi. La commissaire à la protection de la vie privée joue le rôle d'ombudsman dans l'exercice de ses fonctions pour surveiller les pratiques des organisations visées par la LPRPDE en ce qui concerne les renseignements personnels. Si les questions demeurent non résolues, la commissaire peut recourir à la Cour fédérale.

Le modèle d'ombudsman ne date pas d'hier. Les gouvernements s'en servent d'habitude pour réglementer l'administration publique. Ce qu'il y a de novateur dans la LPRPDE, c'est l'application de ce modèle comme moyen de réglementer l'activité du secteur privé. Dans le cadre de ma pratique, je fournis des conseils à une clientèle provenant de tous les secteurs et j'ai eu à travailler et à interagir avec le commissariat; selon mon expérience, le modèle d'ombudsman suivi par le commissariat s'est avéré très efficace et a reçu l'appui général des organisations du secteur privé.

Un modèle d'ombudsman se prête particulièrement bien aux efforts visant à assurer une conformité efficace à la protection de la vie privée. Après tout, pour assurer une protection valable des renseignements personnels, une organisation doit faire plus que simplement respecter les règles juridiques. Il faut plutôt favoriser une mentalité favorable au respect de la vie privée au sein d'une organisation d'une manière qui est adaptée à la réalité du contexte d'affaires de celle-ci. Les directeurs de la protection de la vie ayant de l'expérience comprennent que la vie privée passe par le raffermissement de la confiance. Pour ce faire, il faut une discussion engagée avec les intervenants dans une organisation, dans des secteurs industriels et dans le domaine de la protection de la vie. Le commissariat joue un rôle important dans cette discussion, et le modèle d'ombudsman facilite une interaction flexible et concertée avec les organisations du secteur privé.

La commissaire Jennifer Stoddart a décrit avec éloquence la nature de son rôle à titre d'ombudsman dans un discours qu'elle a prononcé en 2005 sur les mérites de ce modèle. Voici ce qu'elle a dit:

> Plus qu'un moyen de trouver des solutions remédiatrices, les fonctions de l'ombudsman constituent un moteur de changement et d'amélioration. L'objectif consiste bien sûr à résoudre les plaintes mais aussi à établir, grâce à la volonté et à la participation des parties concernées, une culture durable de conscientisation à la protection de la vie privée. Pour atteindre ce but, il faut donc que le processus soit souple, qu'il favorise la participation et qu'il soit adapté à chacun.

Récemment, divers intervenants dans le domaine canadien de la protection de la vie privée, dont la commissaire Stoddart, ont réclamé que la LPRPDE soit modifiée afin d'accorder au commissariat des pouvoirs accrus en matière d'application de la loi. D'après l'expérience que j'ai acquise au cours des 10 dernières années dans le domaine, il n'est pas certain que de telles modifications soient nécessaires.

La commissaire Stoddart et la nouvelle commissaire adjointe, Chantal Bernier, ont remarquablement bien réussi à remplir leur mandat dans le contexte du modèle d'ombudsman, et c'est tout à leur honneur. Elles l'ont fait grâce à une foule de pouvoirs prévus dans la LPRPDE. En particulier, elles ont le pouvoir de nommer publiquement les organisations qui enfreignent la LPRPDE, de lancer de leur propre initiative des enquêtes ou des vérifications concernant les pratiques d'une organisation en matière de renseignements personnels et, comme je l'ai dit, de renvoyer des plaintes à la Cour fédérale.

Le Commissariat à la protection de la vie privée est, depuis des années, très respecté dans le domaine international de la protection de la vie privée, mais il a considérablement amélioré sa réputation auprès des organismes étrangers de protection de données à la suite de son enquête très médiatisée sur les pratiques de Facebook concernant la gestion des renseignements personnels. Grâce aux activités d'application de la loi du commissariat, le Canada est maintenant considéré comme un des chefs de file mondiaux pour ce qui est des questions liées à la protection de la vie privée dans le contexte des nouvelles technologies, y compris des médias sociaux. Le commissariat a accompli ces réalisations sans aucun pouvoir de rendre des ordonnances ou sans aucun autre mécanisme d'application de la loi, comme la capacité d'imposer des amendes. D'ailleurs, la commissaire Stoddart a déclaré à plusieurs reprises que la simple menace publique d'une poursuite possible devant la Cour fédérale contre une organisation a presque toujours amené cette dernière à donner suite aux préoccupations du commissariat.

Les nouvelles technologies innovatrices, comme les plateformes des médias sociaux, procurent de très grands avantages aux Canadiens. À mesure que nous continuerons d'adopter de nouvelles technologies et d'en profiter, nous aurons tous à fournir nos renseignements personnels en cours de route. Voilà pourquoi la protection de la vie privée fera de plus en plus partie intégrante de la relation de confiance entre les organisations du secteur privé et les personnes.

Bien entendu, quand on examine de nouvelles questions en matière de protection de la vie privée, il est important de déterminer si le cadre actuel de réglementation permet d'aborder adéquatement la protection de la vie privée. Avec la LPRPDE, nous sommes chanceux: nous avons un cadre législatif qui est neutre sur le plan technologique, qui repose sur des principes et qui nous a très bien servis pour ce qui est d'assurer une protection de la vie privée de façon équilibrée.

● (1130)

Pour conclure, je présente en toute déférence les suggestions suivantes en espérant que le comité en tiendra compte dans le cadre de son étude, au moment de déterminer la pertinence et l'ampleur des modifications qui s'imposent à la LPRPDE afin de relever les défis posés par les nouvelles technologies, surtout en ce qui concerne les modifications visant à renforcer les pouvoirs d'application de la loi.

Premièrement, en tant qu'individus, nous avons tous la responsabilité de faire attention à la manière dont nous utilisons nos renseignements personnels dans des contextes publics. À cet égard, il est essentiel d'assurer la sensibilisation du public et d'offrir une formation régulière par l'entremise d'organismes de réglementation en matière de protection de la vie privée et des organisations pertinentes du secteur privé. Aucune modification à la LPRPDE ne serait requise pour améliorer nos efforts collectifs en ce sens.

Deuxièmement, je propose respectueusement que le comité examine attentivement les coûts liés à la transition vers un modèle de coercition aux termes de la LPRPDE. Pour tirer parti des nouveaux pouvoirs d'application de la loi comme le pouvoir de rendre des ordonnances, il faudra apporter des changements à la structure du Commissariat à la protection de la vie privée, et on perdra ainsi les principaux avantages fournis par le modèle de l'ombudsman.

Troisièmement, dans le cadre d'une stratégie nationale destinée à assurer la croissance du secteur canadien de la technologie, nous devons bien étudier toute modification ou initiative législative pour éviter d'imposer des obstacles inutiles aux activités commerciales légitimes. Bref, selon moi, il faut examiner soigneusement les coûts économiques associés au changement de la réglementation en matière de protection de la vie privée. Nous avons besoin d'un cadre de réglementation qui favorise l'innovation. Dans le domaine de la protection des renseignements personnels, la LPRPDE nous fournit un modèle approprié qui nous a bien servis jusqu'ici.

Enfin, il faut bien réfléchir aux effets constitutionnels que pourrait avoir tout changement législatif à la LPRPDE, en particulier sur le plan des nouveaux pouvoirs d'application de la loi. Dans l'affaire portant sur la constitutionnalité d'un poste d'administrateur national des valeurs mobilières, la récente décision rendue par la Cour suprême du Canada nous rappelle qu'il faut intégrer les questions constitutionnelles à toute étude sur la réforme législative de la protection de la vie privée.

Merci encore une fois de m'avoir invité à vous parler ce matin. Je serai heureux de répondre aux questions des membres du comité.

[*Français*]

Le président: Je vous remercie.

Nous allons maintenant passer à la période des questions et commentaires.

Monsieur Angus, vous disposez de sept minutes.

[*Traduction*]

M. Charlie Angus (Timmins—Baie James, NPD): Voilà une autre journée de discussion fascinante.

J'aimerais commencer par vous, madame Grimes, parce que, selon moi, ce que vous laissez entendre semble aller à l'encontre du message qui nous a été communiqué, à savoir qu'il est nécessaire de limiter l'accès que les jeunes ont aux médias sociaux, que des limites doivent être établies pour les adolescents âgés de 13 ans ou moins. Je ne connais aucun jeune de moins de 13 ans qui n'utilise pas Facebook ou des médias sociaux. Ils ne sont pas autorisés à consulter YouTube à l'école. Par conséquent, ils sont censés s'abstenir d'utiliser les médias sociaux, mais nous allons créer des petits jardins fermés pour les protéger.

Ces jardins fermés sont exploités par de grandes entreprises qui, selon vos dires, explorent et vendent leurs données, tout en utilisant cet espace à des fins commerciales abusives. Serait-il préférable d'établir des règlements clairs qui visent à limiter la capacité des entreprises à abuser de ce genre de droits et à cibler les renseignements privés des jeunes? Ne devrions-nous pas donner aux jeunes l'accès à des médias sociaux généraux mieux réglementés? Ne serait-ce pas une meilleure solution que ces jardins fermés que les entreprises sont en train d'établir en ce moment?

Mme Sara Grimes: Oui, je le pense. J'ai signalé les deux tendances, mais les deux modèles violent clairement les droits des jeunes et entraînent d'énormes problèmes. Comme vous l'avez dit, les jeunes n'ont pas cessé de se servir de Facebook, parce qu'on leur en a interdit l'accès, et les jardins fermés donnent un faux sentiment de sécurité aux parents et aux jeunes à la recherche de ce genre de solutions de rechange, parce que bon nombre de leurs aspects ne font l'objet d'aucune restriction.

Encore une fois, je ne veux pas dire que tous les sites consacrés aux médias sociaux qui sont conçus précisément pour les jeunes agissent de cette façon dans la même mesure, mais c'est une tendance qui prend un peu d'ampleur avec le temps. Donc, oui, je ne laissais nullement entendre que le fait d'interdire aux jeunes l'accès à certains sites ou de créer des jardins fermés était idéal, mais voilà ce qui s'est passé au cours des 10 dernières années.

C'est un fait, ni l'un ni l'autre des modèles ne fonctionne. Donc, selon moi, nous devons maintenant commencer à chercher des solutions de rechange, à envisager la possibilité de créer un meilleur cadre qui donnerait aux divers fournisseurs de médias sociaux des directives à suivre ou une assise sur laquelle s'appuyer qui ne constitue pas seulement une réaction aux protestations publiques et aux inquiétudes liées aux risques, mais aussi un genre de sensibilité plus générale et plus démocratique à propos de l'ensemble des droits. Je pèserais tous les avantages que les jeunes retirent de leur participation aux médias sociaux et les risques auxquels ces sites les exposent. J'estime que le fait de disposer de ces genres de lignes directrices et de ces cadres aiderait vraiment bon nombre d'entreprises.

● (1135)

M. Charlie Angus: Merci.

Monsieur Kardash, M. Israel et vous avez des points de vue très différents. Il dit que nous devons délivrer des avis de violation et des ordonnances de non-conformité, ainsi qu'imposer des sanctions administratives pécuniaires. En revanche, vous déclarez que le marché fonctionne mieux quand on le laisse faire ce qu'il souhaite et que la commissaire Stoddart est parfaitement satisfaite de la situation.

Vous ne croyez pas qu'il devrait y avoir de meilleures règles en matière de conformité?

M. Adam Kardash: Comme je l'ai mentionné au cours de ma déclaration, la LPRPDE établit, selon moi, un modèle très efficace de protection de la vie privée qui concilie les intérêts des personnes ainsi que ceux des entreprises qui collectent des renseignements et les utilisent dans le cadre leurs activités commerciales.

La commissaire dispose actuellement d'un ensemble de pouvoirs qui, comme les faits l'ont montré au cours des dernières années, lui permettent de régler ces questions avec un succès remarquable, ce qui est tout à leur honneur.

M. Charlie Angus: Quels pouvoirs? Elle affirme que ses pouvoirs sont insuffisants.

M. Adam Kardash: À mon sens, le modèle actuel et les pouvoirs actuels de la commissaire sont parfaitement suffisants.

M. Charlie Angus: D'accord.

J'ai seulement une question à vous poser. Vous n'avez pas mentionné que vous étiez l'avocat de Facebook. Ou, est-ce que cela m'a échappé? Nous avez-vous mentionné que vous représentiez Facebook lorsque vous êtes arrivé ici?

M. Adam Kardash: Je représente tout un éventail d'entreprises du secteur des médias sociaux qui ne font qu'un à ce sujet. Je suis ici seulement à titre privé.

M. Charlie Angus: D'accord.

Donc, monsieur Kardash, M. Israel vous a écrit une lettre le 28 mai 2010. Dans celle-ci, il vous indiquait ce qui suit, en ce qui concerne la façon dont votre client, à savoir Facebook, respectait la LPRPDE.

> nous souhaitons mentionner que la cloison qu'il a l'intention de présenter à ses utilisateurs n'est pas… suffisante pour apaiser les inquiétudes que nous avons signalées à votre client, en ce qui concerne son processus de transition de décembre en matière de protection de la vie privée. Nous soutenons que Facebook n'a pas obtenu le consentement éclairé de ses utilisateurs, dont il a besoin pour procéder à ces changements en matière de protection de la vie privée… la LPRPDE exige que les valeurs par défaut des champs sensibles à la transparence et à la protection de la vie privée cadrent avec les attentes des utilisateurs.

Vous représentiez Facebook dans le cadre d'une affaire très célèbre liée à la conformité. D'après la commissaire à la protection de la vie privée, nous ne semblons pas avoir vraiment réglé cette question.

Ne pensez-vous pas que vous auriez dû mentionner l'entreprise que vous représentez?

M. Adam Kardash: Le Commissariat à la protection de la vie privée a mené de multiples enquêtes ayant trait aux médias sociaux, dont plusieurs liées à Facebook. Selon le Commissariat à la protection de la vie privée, elles ont toutes été résolues de manière satisfaisante. Le personnel du commissariat a examiné attentivement ces questions.

Encore une fois, je ne suis pas ici au nom d'une entreprise en particulier; je suis ici pour représenter un éventail d'entreprises et de points de vue.

M. Charlie Angus: D'accord. Merci.

Monsieur Israel.... Encore une fois, je tiens à préciser que je ne m'en prends pas à Facebook en ce moment. Ce site me plaît. Selon mon épouse en particulier, je lui consacre beaucoup trop de temps. Elle pense que j'ai développé une dépendance à son égard. Je devrais indiquer pour le compte rendu que j'ai peut-être un problème.

Monsieur Israel, vous avez mentionné Acxiom. Vous voyez, nous mettons l'accent sur Facebook, sur Google et sur la question de savoir si, oui ou non, ces entreprises se conforment aux règles. Mais en cette période de grandes collectes de données, il existe des tiers qui explorent les données bien au-delà de ce dont nous avons conscience. Vous avez mentionné cette entreprise appelée Acxiom. Vous avez déclaré qu'elle avait 500 millions de visites à son actif. Nous n'en avons encore jamais entendu parler.

Comment pouvons-nous nous assurer que ces explorateurs de données se conforment dans une certaine mesure aux règles, alors qu'ils passent par…? Il est plutôt facile de collecter simplement d'énormes quantités d'information. Ce n'est pas comme si nous souhaitions nous acharner sur Facebook ou sur Google; il y a des entreprises qui recueillent ces renseignements, et nous ignorons totalement qu'elles existent. Quelles mesures devons-nous prendre pour nous occuper de ces entreprises?

● (1140)

M. Tamir Israel: Eh bien, c'est assurément un secteur qui pose des difficultés. Je suis d'accord avec Adam lorsqu'il dit que nous devrions mettre en oeuvre des régimes souples qui ne font pas obstacle aux innovations véritables et aux initiatives de ce genre. J'utilise également Facebook, et ses services me plaisent.

Je pense qu'il y a un écart entre ce que les utilisateurs pensent qu'il se produit lorsqu'ils conversent avec leurs amis et leurs collègues dans ces sites en ligne et la façon dont l'information circule. Bon nombre d'échanges liés aux médias sociaux ont lieu dans un environnement semi-public, et des entreprises comme Acxiom sont essentiellement libres de saisir les renseignements échangés et de les stocker dans leurs bases de données. Cela déroge probablement aux conditions d'utilisation de Facebook, mais il n'y a aucune transparence dans ce processus. Personne ne suit très attentivement la façon dont l'information est acheminée dans ces bases de données et les règles qui régissent cette collecte.

En ce qui a trait en particulier aux courtiers en information de ces bases de données, c'est un environnement qui présente des défis, car ils ne traitent pas directement avec les utilisateurs. Par conséquent, vous devez… La FTC songe à mettre en vigueur certaines règles qui encourageront l'industrie à créer des sites centralisés que les utilisateurs pourront consulter afin de vérifier si les courtiers en information possèdent un dossier sur eux et, le cas échéant, de déterminer les renseignements qu'ils détiennent et leur provenance.

Ce pourrait être un début. Nous n'avons pas besoin d'amendes très sévères ou de quoi que ce soit du genre, dans ce contexte. Toutefois, pour obtenir une conformité tant proactive et que réactive, il est absolument nécessaire de les menacer de sanctions, s'ils continuent d'ignorer les principes qui existent. Je ne dis pas que ce sont tous des mauvais joueurs mais, s'ils ne risquent pas de recevoir une sanction, peu de choses les inciteront à découvrir en quoi consistent ces principes sur le plan pratique et à les intégrer dans leur modèle d'affaires.

M. Charlie Angus: Ce qui me préoccupe, c'est que…

[*Français*]

Le président: Malheureusement, votre temps de parole est écoulé.

[*Traduction*]

M. Charlie Angus: Je ne faisais que commencer, monsieur le président.

[*Français*]

Le président: Vous en êtes déjà presque à neuf minutes.

Je vais maintenant céder la parole à M. Calkins, pour sept minutes.

[*Traduction*]

M. Blaine Calkins (Wetaskiwin, PCC): Merci, monsieur le président.

Je remercie infiniment nos témoins de leur présence. Nous avons entendu des témoignages fascinants aujourd'hui.

J'ignore par où commencer, mais je vais simplement commencer par vous, madame Grimes.

Vous avez dit qu'à l'insu de la plupart des Canadiens — je pense que ce fait est assez connu —, leurs activités en ligne sont surveillées. Il y a des explorateurs de données, des aspirateurs de site et des robots qui interviennent sur Internet. Les gens téléchargent involontairement dans leur ordinateur toutes sortes de logiciels. Des logiciels espions, des logiciels malveillants, des logiciels de publicité, ou peu importe comment vous voulez les appeler, suivent les activités des gens, qu'ils utilisent un ordinateur portatif ou un dispositif mobile. Dans les contrats d'utilisation, nous acceptons que nos renseignements soient employés. Les paramètres de nos appareils nous permettent d'autoriser ou non les témoins, par exemple, dans nos ordinateurs. Ces paramètres existent dans nos iPods et nos iPads. Nous recevons des avis de diffusion personnalisée, et nous pouvons activer ou désactiver ces paramètres. Un utilisateur informé devra déployer quelques efforts pour y arriver. Nous pouvons nous procurer des logiciels tiers qui nous aideront à protéger, par exemple, nos ordinateurs à la maison que nos enfants utilisent pour tenter de faire leurs devoirs. Ainsi, en tant que parent, je peux être informé du genre d'activités que mes enfants pratiquent ou non en ligne.

Voilà l'une des questions que j'aimerais vous poser. Croyez-vous que mon enfant a le droit d'utiliser un ordinateur pour s'adonner à certaines activités, sans que je le sache? Je vais garder cette question pour la fin.

En ce qui concerne tous les contrats, soit j'en accepte toutes les conditions, soit je les refuse en bloc. C'est le seul choix qui s'offre à moi. Je n'ai pas la possibilité d'analyser le contrat et d'en refuser certaines parties.

Ma question, que j'adresse en général à vous trois, est la suivante: selon vous, une loi ou un règlement devrait-il exiger que ces genres de contrats d'utilisation puissent être analysés de sorte que l'utilisateur final ait, en fait, le pouvoir de sélectionner les parties auxquelles il consentira ou non? La plupart de ces contrats décident par défaut de la façon dont mes renseignements personnels seront partagés avec des entreprises comme Acxiom, ce qui me terrifie, pour être honnête.

Je sais comment ces choses fonctionnent parce que, dans le passé, j'étais un administrateur de base de données. Je comprends comment ces points de données sont collectés, et bon nombre d'entre eux le sont à mon insu. Je suis certain que mon nom se trouve dans la base de données d'Acxiom ou, sinon, dans celle d'une autre entreprise. Quelqu'un possède des renseignements à mon sujet, au sujet de mes habitudes d'utilisation et de navigation, etc. Je trouve donc cela très frustrant.

Pourquoi, en tant qu'utilisateur, n'ai-je pas le pouvoir de choisir les parties du contrat auxquelles je consens ou non? Est-il raisonnable, sur le plan de la réglementation, que le gouvernement intervienne en ce sens?

● (1145)

Mme Sara Grimes: Pour les parties plus générales de la question, je vais m'en remettre aux autres témoins ici présents.

En ce qui concerne les contrats à l'intention des jeunes et des utilisateurs, il faut vraiment que des changements leur soient apportés. J'ai lu de nombreux contrats de licence d'utilisation conçus pour des services destinés à des jeunes. Ils comportent tous les mêmes genres de clauses que l'on retrouve dans ces documents, quels qu'ils soient. Toutefois, il y a toutes sortes de complications lorsque des jeunes sont en cause. Ces contrats contiennent des mots dont les jeunes ne peuvent pas comprendre la signification et que même la majorité des adultes ont du mal à saisir. Les contrats de service décrivent les relations avec des termes que les jeunes ne sont pas encore en mesure de comprendre. Il faudra qu'ils vieillissent encore un peu avant de pouvoir saisir des concepts aussi complexes que des échanges de biens et divers processus économiques qui sont décrits comme des services ou des utilisations.

Il est absolument nécessaire de modifier les mots employés dans les contrats de services destinés aux jeunes, dans lesquels je me spécialise, de sorte qu'ils soient compréhensibles tant pour les jeunes que pour les parents. J'estime que notre pays, notre gouvernement doit commencer à réfléchir à la façon dont nous allons gérer le fait que des jeunes signent des contrats, parce que les contrats mettant en cause des mineurs sont très épineux sur le plan juridique. Ils sont résiliables, et il y a toutes sortes d'étranges précédents à prendre en considération.

Je ne suis pas une experte en matière de droit, mais, juste à penser au degré de complexité que la situation prendra si on la considère sous ce jour, j'attrape un mal de tête. Toutefois, nous devons commencer à nous attaquer à cette question, à y réfléchir sérieusement et à penser aux conditions de service que nous prévoyons que les jeunes satisferont lorsqu'ils signent des contrats de 15 pages truffés de toutes sortes de jargons, qui décrivent des processus qui dépassent tellement leur entendement qu'on ne peut raisonnablement s'attendre à ce que ces contrats soient honorés.

Donc, oui, j'aimerais que les conditions de service des contrats d'utilisation soient mieux adaptées, que certains des mots employés soient des termes qui ont été jugés appropriés pour des jeunes, et qu'un cadre soit établi pour déterminer comment nous allons gérer la question de la personne qui signe le contrat et qui accepte de respecter ses clauses et du degré de participation des parents, parce qu'il est clair qu'ils devront jouer un rôle dans ce processus.

M. Blaine Calkins: Merci.

M. Adam Kardash: C'est une excellente question, car elle illustre comment il est impossible de parler de la vie privée de façon significative avec seulement un processus de consentement préalable, en particulier pour les tribunes qui deviennent plus complexes.

Il y a deux façons de composer avec toutes sortes de contextes, non seulement dans le secteur de la technologie pure, mais à plus grande échelle encore. La première est que, en plus d'un préavis concernant les engagements que l'utilisateur devrait prendre, en réalité la chose la plus importante est maintenant en deux volets. Une partie consiste à s'assurer que les utilisateurs ont le contrôle approprié et qu'ils savent où exercer ce contrôle. L'autre — et c'est un point absolument essentiel et le thème qui est ressorti de la pratique au cours des dix dernières années — est que nous sommes passés du point où les concepts du consentement et du préavis étaient des parties importantes de la protection de la vie privée à celui où l'on privilégie le concept de la gouvernance en matière de protection de la vie privée et une approche beaucoup plus holistique de la façon de traiter ces questions.

Je crois qu'il y a deux ou trois semaines, le Commissariat à la protection de la vie privée du Canada et les organes de réglementation de la vie privée en Alberta et en Colombie-Britannique ont publié un document d'orientation conjoint de 26 pages concernant leurs attentes, s'agissant des programmes efficaces de gestion de la protection de la vie privée. Ces attentes sont assorties d'obligations pour les organismes d'examiner les questions de vie privée en se distanciant de toute la gamme du cycle de vie des données mais du point du vue du risque, de façon à continuellement améliorer leurs pratiques et à traiter de sujets comme les contrôles et la transparence. Par-dessus tout, ils traitent la question beaucoup plus en détail.

J'encourage le comité à se reporter à ce document. Il y au moins 110 attentes qui vont au coeur de votre question. Si les entreprises dépendent exclusivement de ces formulaires de consentement interminables... J'avais l'habitude de rédiger ces choses. Je sais de quoi elles traitent. Elles ne sont pas efficaces pour ce qui est de la conformité à la protection de la vie privée. C'est la gouvernance en matière de protection de la vie privée qui est exactement au coeur de la question que vous avez soulevée.

● (1150)

M. Tamir Israel: C'est une excellente question. Je suis bien d'accord pour dire qu'il est important d'en faire un petit peu plus pour simplifier les politiques relatives à la protection de la vie privée. Il a été question de tenter de normaliser certains termes qui ont des significations semblables pour diverses entreprises, mais qui sont décrits différemment, pour faire en sorte qu'il soit plus facile pour les consommateurs de comparer les politiques en matière de protection de la vie privée, mais je suis d'accord avec mon collègue que le processus ne peut pas en finir là.

Il est très important d'être responsable et de faire en sorte que les organismes mettent en place des processus qui tiennent compte des préoccupations en matière de protection de la vie privée à tous les stades de l'élaboration de leurs services. Je crois que notre commissaire fédéral à la vie privée et certains de ses homologues provinciaux ont fait du très bon travail pour instaurer ces mesures.

Par contre, il est très important de s'assurer que l'essence de ce qui est intégré à ces processus d'élaboration reflète aussi les attentes et la vie privée de nos utilisateurs. Il y a toujours eu un clivage à l'échelle internationale entre ce que l'Union européenne, le Canada et les États-Unis font. Les États-Unis avaient un type de cadre ouvert dans lequel il n'y avait pas beaucoup de réglementation, mais ils s'éloignent beaucoup de ce modèle pour s'approcher du point où nous sommes et pour aussi adopter ces types d'avis in extremis juste-à-temps par lesquels vous offrez plus de préavis et plus de contrôle à l'égard des décisions que vous prenez. Cela aide à ajuster les éléments de la politique en matière de protection de la vie privée pour permettre aux utilisateurs d'avoir un meilleur contrôle des parties qu'ils approuvent et des parties qu'ils n'approuvent pas.

[*Français*]

Le président: Merci, monsieur Calkins.

[*Traduction*]

M. Blaine Calkins: Il me reste deux ou trois minutes, monsieur le président.

[*Français*]

Le président: Malheureusement, votre temps de parole est écoulé, monsieur Calkins.

Bien que ce soit très intéressant, je dois laisser la parole à M. Andrews, pour sept minutes.

[*Traduction*]

M. Scott Andrews (Avalon, Lib.): Merci, monsieur le président.

Monsieur Calkins, je vais essayer de revenir à vos questions concernant les parents et le rôle des enfants dans tout cela.

Sara, ma question s'adresse à vous. Il y a des enfants qui sont nés aujourd'hui et qui ne connaîtront que Facebook. Ils vont grandir. Nous nous trouvons à un stade critique aujourd'hui, car ces enfants prennent maintenant conscience de ce qu'est Facebook.

En tant que parents, nous aimons parfois parader nos enfants, et nous les mettons sur Facebook avant même qu'ils viennent au monde. Pas plus tard qu'hier, j'ai vu une photo d'écographie sur Facebook.

Quel rôle les parents ont-ils à jouer dans ce débat? Nous le commençons parfois même avant leur naissance. Ensuite, une fois qu'ils sont nés, nous étalons leur vie. Je crois que nous sommes en partie responsables ici.

Y a-t-il de la sensibilisation à faire dans ce cas? Y a-t-il une façon de stopper ce génie ou est-il déjà sorti de sa lampe sans que l'on puisse retourner en arrière?

Mme Sara Grimes: Cela dépend à quoi le génie correspond, je suppose, pour ce qui est de la vie publique et en ligne. C'est difficile de savoir si c'est même quelque chose que nous devrions tenter de prévenir et d'interdire. Nous essayons de trouver la meilleure façon de procéder, la meilleure façon d'accueillir les enfants dans ce monde dans lequel ils naissent. Il n'y a pas vraiment de solution de rechange. Ils ont des leçons et des devoirs qui les amènent vers les médias sociaux. Bien de l'interaction sociale se fait à cet endroit. Il y a des occasions d'être politique, de se renseigner au sujet d'événements importants. Il y a une tonne d'avantages. Selon moi, ce qui importe, c'est la façon dont vous mettez en équilibre les avantages et les risques, au lieu de seulement vous arrêter à l'un ou à l'autre.

Pour ce qui est de la participation des parents, les jeunes enfants et les parents forment souvent une unité. Il s'agit de processus familiaux que les familles traversent ensemble. La façon dont les familles les négocient est vraiment importante, mais il ne peut entièrement leur revenir de prendre ces types de décisions. Comme vous le dites, ce ne sont pas tous les parents qui savent tout ce qu'il y a à savoir. C'est un secteur nouveau où tout bouge vite. Les gens ont du mal à suivre. C'est beaucoup demander aux parents de surveiller et de réglementer la moindre petite chose que font leurs enfants. S'ils se déchargent de cette responsabilité sur un genre de programme de cybergardienne, un certain nombre de ces programmes ont fait l'objet d'enquêtes pour avoir fait énormément de forage de données concernant les enfants qu'ils protègent de certains sites et tout cela.

Traiter cette question dans une optique familiale est vraiment une façon utile d'y penser, mais les familles ont aussi besoin d'appui. Elles ont besoin de lignes directrices. Elles ont aussi besoin d'avoir des experts, des politiciens et des avocats de leur côté pour penser à la meilleure façon de gérer ces choses et d'appuyer les pratiques exemplaires qui ressortent et de ne pas laisser aux familles la lourde responsabilité de trouver des solutions à des problèmes très complexes.

● (1155)

M. Scott Andrews: Il arrive souvent que les gens s'en remettent entièrement au gouvernement, et cela a été fait au fil des ans. Voilà pourquoi nous avons un âge légal pour boire et un âge légal pour fumer. Nous sommes donc en droit de nous demander si nous avons besoin d'imposer une limite d'âge dans ce cas et, dans l'affirmative, est-ce impossible à contrôler, et avons-nous déjà dépassé le stade de le faire?

Mme Sara Grimes: C'est un peu embêtant de comparer cela à quelque chose comme l'alcool, parce qu'il est prouvé que l'alcool présente des risques pour la santé. Il a des effets néfastes sur le développement mental et physique et peut causer toutes sortes de graves problèmes aux jeunes enfants s'ils en consomment trop tôt. Je vois le cyberespace comme un espace public. Nous n'avons pas de limites d'âge pour les espaces publics, les parcs et les rues. Les enfants ont le droit de sortir en public. Si l'on pense au cyberespace comme d'un prolongement de l'espace public, il sera vraiment problématique, selon moi, d'y imposer une limite d'âge.

Cela ne signifie pas que nous ne pouvons pas avoir de règlements et de lois qui orientent ces pratiques et qui prévoient la façon d'aborder et de traiter les enfants. Il y a des parties du cyberespace public qui sont vraiment inappropriées. Je pense à des exemples extrêmes ici, comme dans notre monde physique, nous ne laisserions pas les enfants entrer dans certains magasins et à certains endroits. Alors je crois qu'il serait possible d'appliquer les mêmes types de règles et d'approches plus nuancées et plus raisonnées à ce contexte au lieu de limites d'âge. Elles fonctionnent rarement en ligne, car elles placent beaucoup de responsabilité sur les enfants et les familles.

Voilà pourquoi je crois que la loi sur la protection en ligne de la vie privée des enfants a été jugée... Je ne crois pas que cette loi aux États-Unis soit un échec complet. Je crois qu'elle a généré bien des choses positives. D'autres personnes ont jugé qu'elle était un échec, car les enfants sont capables d'outrepasser les limites d'âge. Peut-être qu'elle privilégie une approche trop générale, et elle place aussi la responsabilité de toute la surveillance sur les enfants et les parents. La limite d'âge est bien là, et s'ils ne la respectent pas, alors ils sont punis en quelque sorte.

M. Scott Andrews: Nous nous occupons de nos mineurs, et ils sont visés par des lois. Comment des parents comme M. Calkins et moi-même pouvons-nous intervenir dans tout cela? Avons-nous le droit de prendre contact avec ces entreprises et de dire: « Mon enfant est en ligne et j'ai besoin de faire quelque chose, de surveiller ce qu'il consulte »? Est-ce une responsabilité? Est-ce une chose qui devrait nous préoccuper en tant que parents?

Mme Sara Grimes: Un des aspects très positifs, en fait, de la loi sur la protection en ligne de la vie privée des enfants était qu'une partie stipulait que les parents avaient le droit de prendre contact avec les entreprises, de connaître toutes les données que l'entreprise avait recueillies concernant leur enfant et de demander qu'elles soient détruites. Selon les personnes qui ont fait un suivi et examiné la façon dont la loi a bien ou mal fonctionné au cours des 10 ou 12 dernières années, c'est quelque chose qui n'a pas été fait très souvent. Mais c'était une façon de procéder. On présume que les enfants pourraient aussi exiger la même chose et connaître les données qui ont été recueillies sur eux et avoir un type de recours, une solution établie, pour faire en sorte que les données soient détruites s'ils le souhaitent.

M. Scott Andrews: Vous avez dit qu'il s'agissait de la loi sur la protection en ligne de la vie privée des enfants?

Mme Sara Grimes: Oui, aux États-Unis.

M. Scott Andrews: D'accord.

J'aimerais demander à M. Kardash comment cela concorde avec notre LPRPDE. Voyons-nous les choses du même oeil?

M. Adam Kardash: Le Canada n'a pas de loi qui vise précisément la protection de la vie privée des enfants, mais implicitement... Dans la LPRPDE il y a, entre autres, des règles relatives au consentement. Les enfants, et certainement ceux de moins de 13 ans, n'auraient pas la capacité légale de donner leur consentement. Dans le contexte de certaines activités qu'ils feraient, le consentement d'un parent ou d'un tuteur serait nécessaire pour qu'ils puissent légalement le faire. Alors, dans cette optique, le parent se met à la place de l'enfant.

Nous avons des dispositions qui sont probablement plus sévères que celles de la loi sur la protection en ligne de la vie privée des enfants, car en plus des règles régissant le consentement, nous avons toute une gamme d'autres exigences auxquelles un organisme aurait encore à se conformer — la sécurité, le préavis aux parents, les pratiques de conservation et de destruction des renseignements personnels, et les droits d'accès qui seraient donnés à chaque parent.

Alors vous avez tout un complément d'obligations juridiques qui suffiraient toujours, mais fondamentalement vous avez cette disposition relative au consentement qu'un enfant de moins de 13 ans n'aurait pas la capacité légale de donner.

M. Scott Andrews: Dans quelle mesure est-il difficile pour...

● (1200)

[*Français*]

Le président: Merci. Votre temps de parole est malheureusement écoulé, monsieur Andrews.

Pour que ce soit égal, il faut que tout le monde dispose du même temps de parole.

Madame Davidson, vous disposez de sept minutes.

[*Traduction*]

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

Un grand merci à chacun de nos invités d'aujourd'hui. C'est un sujet extrêmement intéressant que nous étudions ici. Je crois que les commentaires que vous formulez aujourd'hui soulèvent beaucoup plus de questions et de préoccupations que ce que nous devons traiter.

En particulier, madame Grimes, vous avez parlé de certains des sites pour enfants et de certaines des choses auxquelles ils ont accès. Je crois que vous avez dit que leur droit à la vie privée peut être enfreint à des fins commerciales par certaines de ces entreprises. Vous avez parlé des mécanismes de protection mis en place dans d'autres pays. Certaines régions ont une interdiction, pour les moins de 13 ans, de visiter certains sites.

Je suis d'accord, je pense que les consentements qui sont exigés aujourd'hui ne conviennent pas du tout aux enfants. Je crois qu'ils ne conviennent pas non plus aux adultes dans la plupart des cas. Je n'arrive pas à comprendre comment une personne puisse être assurée que parce que les enfants de moins de 13 ans sont visés par une interdiction, celle-ci puisse être appliquée. Ce que je veux dire, c'est que n'importe qui peut affirmer qu'il a 13 ans ou plus. Si un enfant est déterminé à visiter un site parce que ses pairs le font ou pour toute autre raison que ce soit, il dira qu'il a plus de 13 ans. Je crois que c'est tout simplement ridicule de même penser que cela pourrait rassurer quelqu'un.

Je me demande si vous pourriez parler un peu des autres pays. Vous avez parlé brièvement des États-Unis et de certaines des mesures de protection qu'ils ont mises en place. Y a-t-il des mesures prises dans d'autres pays que nous pourrions examiner?

Par ailleurs, avez-vous des exemples de réseaux sociaux dans lesquels les enfants sont précisément ciblés et peut-être exploités à des fins commerciales? Et pensez-vous que les enfants eux-mêmes se préoccupent de leurs droits à la vie privée?

Mme Sara Grimes: Il y a eu des développements et des recommandations au sein de l'Union européenne. Je ne suis pas suffisamment à jour pour savoir où ils en sont rendus dans ce processus. Ils ont mené une très grande étude à l'UE, qui s'est terminée récemment. Les universitaires et un certain nombre d'organismes gouvernementaux ont étudié ces types de questions avec des enfants de divers âges qui utilisent Internet dans le cadre du projet EU Kids Online. Après la parution des rapports, je sais que l'on a entamé des discussions concernant les lignes directrices de l'industrie et la mise en oeuvre de nouvelles lignes directrices et d'une réglementation éventuelle. Je ne sais pas exactement où ils en sont rendus dans ce processus, mais ce serait un endroit où regarder. Je sais qu'ils l'envisagent, et ils ont aussi appuyé une grande partie de ce qu'ils font sur des projets de recherche, ce qui est fantastique.

Pour ce qui est des exemples d'enfants qui sont précisément ciblés et exploités à des fins commerciales, un des gros problèmes que pose l'étude de ce secteur et de ces processus est le manque de transparence. Les données sont recueillies, et vous pouvez lire les conditions de service et voir, en quelque sorte, que les données viennent de différentes sources, mais on ne voit pas toujours clairement quels sont les liens et la façon dont les données sont transférées et utilisées. Les exemples que j'ai examinés pour comprendre le fonctionnement de ce processus sont surtout des sites qui vendent les données à d'autres entreprises et qui ne se cachent pas de le faire. Ils fonctionnent comme un espace de média social, mais ils font aussi du forage et du courtage de données maison.

Un exemple d'il y a quelques années était celui de Neopets, qui est une communauté en ligne pour les enfants. Ils ont vendu l'étude de marché qu'ils avaient réalisée à diverses entreprises et ils publiaient un rapport annuel dans *AdAge*, qui est une grande revue spécialisée de l'industrie de la publicité aux États-Unis. Ils fournissaient des enquêtes et des stratégies d'études de marché assez faciles à reconnaître dans ce site.

Un exemple plus récent est celui de Habbo Hotel, dont la base est en Finlande, mais qui est populaire dans le monde entier. La plupart des gens qui l'utilisent ont entre 13 et 18 ans, je crois, mais ils ont aussi un nombre considérable d'utilisateurs entre 11 et 13 ans. Ils offrent un type de service semblable, appelé Habbel, par l'intermédiaire duquel ils compilent les données et les vendent à d'autres entreprises. Les entreprises peuvent aussi faire appel à Habbel à l'avance pour, en quelque sorte, espionner les conversations que les enfants pourraient avoir au sujet d'un produit en particulier et leur rapporter non seulement ce que les enfants disent concernant le produit, mais aussi le contexte général dans lequel cette conversation a lieu — leurs goûts, les parties du site autour desquelles ils gravitent, les autres sujets qu'ils abordent, l'heure à laquelle ils vont sur le site, où ils prévoient d'aller par la suite s'ils décident de se rencontrer en personne, car bien des enfants qui se communiquent par le biais des médias sociaux se connaissent aussi dans la vraie vie et ils fréquentent les mêmes écoles et ce type de choses. Il peut s'agir d'informations très détaillées.

La seule raison pour laquelle nous savons à quel point elles sont détaillées et nous sommes au courant de ces types de processus est qu'ils vendent leurs données ouvertement. Mais dans bien des cas, ils ne les vendent pas. Ils les conservent ou ils les vendent de façon beaucoup plus dissimulée, alors c'est moins évident.

Les enfants se préoccupent-ils de la protection de la vie privée? Tout à fait. On a beaucoup parlé des différentes conceptions qu'ils ont de la vie privée. Je crois que cela nous ramène au commentaire qu'a formulé M. Andrews un peu plus tôt concernant les enfants nés à l'âge de Facebook, qui ne connaissent rien d'autre et dont les photos sont affichées en ligne avant qu'ils soient assez vieux pour y aller eux-mêmes.

Il est possible que leurs conceptions de la vie privée diffèrent légèrement, mais une bonne partie d'entre elles ressemblent beaucoup aux conceptions traditionnelles. Au fil des études, ce qui ressort le plus est qu'ils se préoccupent surtout des atteintes à la vie privée qui influent directement sur eux: les amis ou les parents qui portent atteinte à leur vie privée ou la perception que leurs parents le font. Ces formes abstraites sont détaillées. Elles ne semblent pas influer sur eux quotidiennement. Ils traitent ces questions de protection de la vie privée d'une façon que nous ne comprenons pas encore entièrement. Ils peuvent ne pas sembler aussi préoccupés par ces choses, mais il arrive souvent qu'ils ne comprennent pas vraiment comment et où elles peuvent les toucher. Honnêtement, puisque bon nombre d'entre nous ne comprennent pas non plus comment ces types d'atteintes à la vie privée influent sur nous et à quel endroit, nous nous inquiétons de ce qui pourrait arriver, mais nous ne voyons pas encore entièrement les conséquences. C'est plus difficile de savoir ce qu'ils en pensent.

● (1205)

Il y a une nouvelle étude sur les enfants et les jeunes Canadiens qui vient de paraître et qui porte sur ces questions. Les enfants sont de plus en plus capable d'exprimer des préoccupations concernant la nature abstraite de l'atteinte à la vie privée, ce qui, selon moi, est un développement très important. Ils en apprennent plus à ce sujet, ils en font davantage l'expérience et ils sont plus capables de dire comment ils se sentent à ce sujet et s'ils estiment que l'on porte atteinte à leurs droits.

Ce qui est triste, c'est que je ne suis pas sûre qu'ils estiment avoir une porte de sortie, une solution ou une solution de rechange. On ne leur en présente certainement pas à l'heure qu'il est.

[*Français*]

Le président: Votre temps est écoulé, puisqu'il inclut la question et la réponse.

Madame Borg, vous avez cinq minutes.

Mme Charmaine Borg (Terrebonne—Blainville, NPD): Je remercie les témoins d'être ici aujourd'hui.

Ma première question s'adresse à M. Israel. Selon ce que j'ai lu, lorsque la commissaire fait des recommandations concernant la politique de protection de la vie privée, certaines compagnies changent complètement d'interface pour rendre ces recommandations désuètes.

Pouvez-vous faire des commentaires là-dessus? Cela pourrait-il justifier le fait que la commissaire ait besoin de plus de pouvoirs pour imposer des sanctions pécuniaires?

[*Traduction*]

M. Tamir Israel: Merci, c'est une très bonne question.

Je crois que dans bien des contextes, l'industrie observe les règles, mais le problème est qu'il arrive parfois que, dans le contexte des réseaux sociaux et d'Internet, certains des mécanismes nécessaires pour se conformer à la recommandation de la commissaire à la protection de la vie privée soient longs à mettre en oeuvre — à élaborer et à mettre en place. Nous l'avons vu aux États-Unis avec la Federal Trade Commission dans un certain nombre de plaintes liées à la vie privée qu'ils ont examinées. Nous l'avons vu dans certains cas au Canada.

Le problème est que le mécanisme que nous avons mis en place en application de la LPRPDE ne permet pas vraiment à la commissaire à la protection de la vie privée de contrôler cette question en permanence. Quatre-cinq jours après la mise en oeuvre de cette recommandation, ils doivent décider de porter la question devant la Cour fédérale — de recommencer à zéro et de le faire dans le contexte d'un procès, ce qui n'est pas un contexte très souple pour faire de la gouvernance en matière de vie privée — ou de prendre des arrangements vraiment indéfinis.

Dans une affaire que nous avons eue, il s'agissait presque d'une entente contractuelle qui avait été signée avec la partie. Aux États-Unis, vous voyez des choses semblables, à savoir des conventions de règlement entre la Federal Trade Commission et les entreprises pour faire certaines choses sur un certain nombre d'années. Mais il n'existe pas nécessairement de mécanismes d'application et de processus bien définis pour traiter ces types de processus de conformité.

● (1210)

[*Français*]

Mme Charmaine Borg: Merci beaucoup.

Est-ce qu'il arrive que des entreprises changent complètement leur interface pour éviter la mise en oeuvre de certaines recommandations? Est-ce un problème?

[*Traduction*]

M. Tamir Israel: Je dirais que cela est ennuyeux, oui, mais ce l'est en partie parce qu'il s'agit d'un problème à deux niveaux. Ces sites évoluent si rapidement qu'il est difficile de... Vous avez besoin de quelque chose de plus souple pour que le commissaire à la protection de la vie privée puisse s'adapter. Six mois en temps Internet équivaut à une décennie en temps normal, il faut donc un processus pour que la commissaire à la protection de la vie privée puisse adapter, en continu, l'intention de leur principe, car ce qui arrive souvent, c'est que, le temps qu'une réponse soit mise en place, elle finit par faire le contraire de ce qu'elle devait faire, par exemple.

[*Français*]

Mme Charmaine Borg: Merci.

Monsieur Kardash, voulez-vous faire des commentaires?

[*Traduction*]

M. Adam Kardash: Puis-je formuler un commentaire? Pour vous mettre un peu en contexte, j'ai eu l'occasion de représenter des entreprises de tous les secteurs dans le cadre de multiples enquêtes au sein du Commissariat à la protection de la vie privée du Canada. Du moins d'après ce que j'ai constaté, une fois qu'une enquête a été lancée, les entreprises finissent toujours par trouver — ou ont trouvé — une solution adaptée à leurs pratiques commerciales, mais à la satisfaction du commissariat.

Comme je l'ai mentionné dans mes remarques liminaires, la commissaire Stoddart a dit officiellement que la simple menace d'une action devant la Cour fédérale a été très efficace. Rien n'est plus important pour la plupart des entreprises — voire toutes les entreprises — que leur réputation. La perspective d'être nommées publiquement est une chose qu'elles veulent vraiment éviter, alors elles se conforment.

[*Français*]

Mme Charmaine Borg: Merci.

Monsieur Israel, vous avez donné l'exemple d'Acxiom, qui a amassé une grande quantité de données.

Devrait-on penser à établir des principes pour minimiser la quantité de données que les compagnies sont en train d'amasser? Comment pourrait-on mettre cela en pratique maintenant?

[*Traduction*]

M. Tamir Israel: C'est une très bonne question. Je pense que cela doit être examiné de plus près.

La même question commence à être soulevée dans le contexte des jeux électroniques pour enfants. Avant, les documents de marketing étaient plus faciles à obtenir parce que les entreprises y décrivaient leurs pratiques. Si j'essayais de comprendre ce qu'un site précis faisait, je pouvais consulter leurs documents de marketing et y trouver la réponse, comme le disait Sara. Maintenant, ils ne le font plus. Ils ne mettent plus ces documents à disposition, alors ce n'est plus aussi facile d'obtenir l'information.

Il en va de même pour les courtiers de données. Je ne sais pas vraiment ce qu'ils font. Vous pouvez consulter certains de leurs documents de marketing pour vous faire une idée, mais je crois que vous avez besoin... Je n'ai pas de solution. Je crois qu'il faut procéder à un examen plus approfondi, en compagnie de ces courtiers, pour essayer de les convaincre d'expliquer en quoi consistent leurs processus.

Il a été suggéré de n'avoir qu'un endroit centralisé où les personnes peuvent envoyer un message à ces courtiers de données et faire des recherches à leur sujet dans un seul et même endroit pour voir si leurs noms s'y trouvent. Ensuite, vous avez, en vertu de la LPRPDE, par exemple, le droit de demander à un organisme de vous donner tous les renseignements qu'il a sur vous. Mais vous devez d'abord savoir vers quel organisme vous tourner, quels sont les organismes. Je ne veux pas envoyer 100 000 demandes du genre. S'il y a 100 000 courtiers de données, je veux pouvoir aller à un seul endroit, voir qui ils sont, leur envoyer une demande, voir quelles données ils ont sur moi et, ensuite, peut-être corriger des erreurs éventuelles qui se trouvent dans ces documents.

En plus de ce mécanisme de transparence, il existe peut-être aussi un genre de mécanisme de réglementation analogue qui pourrait être mis en place pour parler à ces organismes et avoir une idée de l'endroit où ils envoient leurs données, de la façon dont ils les utilisent et de la source à laquelle elles sont puisées. C'est un genre de mission d'information qui, selon moi, serait vraiment utile, mais c'est très difficile pour les particuliers d'entreprendre la leur.

C'est un point de départ.

● (1215)

[*Français*]

Le président: Merci. Votre temps est écoulé.

Je cède la parole à M. Butt, pour cinq minutes.

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

[*Traduction*]

Un grand merci à tous les témoins d'être venus. Je crois que les autres membres du comité l'ont bien dit, la journée est pleine d'enseignements. Je vous sais gré de votre expertise en la matière.

Je vais vous proposer un concept pour savoir ce que vous en pensez. Je vais l'appeler, faute de mieux, une option de facturation négative inversée en ce qui concerne la protection de la vie privée ou le formulaire de consentement. Serait-il possible, ou faisable selon vous, que, à moins qu'un utilisateur donne expressément son consentement à ce que l'entité — Facebook, Google, qui que ce soit — détienne ses renseignements personnels et les diffuse ensuite, au lieu de consentir expressément à ce qu'ils soient utilisés...?

Je crois comprendre que les politiques en matière de protection de la vie privée stipulent, en gros, qu'ils peuvent utiliser tous ces renseignements à leur guise. Vous cliquez sur « J'accepte ». Personne ne lit les 15 pages. Vous cliquez simplement sur « J'accepte » parce que vous voulez vous inscrire.

Est-ce que cela peut fonctionner dans l'autre sens? Pouvons-nous l'établir... que ce soit par l'intermédiaire du Parlement dans nos règlements ou nos lois, ou par l'intermédiaire d'une entente entre les entreprises? Je vais parler de votre modèle d'autoréglementation dans un instant, ce sera ma question de suivi. Pouvons-nous exercer des pressions sur ces entreprises — et serait-il possible — d'avoir une politique en matière de protection de la vie privée qui fonctionne dans l'autre sens? Par exemple, « vous n'êtes autorisé à utiliser mes renseignements personnels sous aucun prétexte à moins d'obtenir mon consentement exprès ». Est-ce une option viable? Fonctionnerait-elle?

M. Tamir Israel: Je suis d'accord avec ce que mon collègue, M. Kardash, a dit tout à l'heure, que vous avez besoin de mettre en place un cadre souple. Nous avons besoin d'un régime de consentement au Canada; alors, au départ, ils ont techniquement besoin de mon consentement. C'est un régime de consentement graduel dans lequel plus les renseignements sont confidentiels en ce moment, au sens de la LPRPDE, plus le consentement demandé doit être explicite — en théorie. Le problème est qu'il a été très difficile de transposer ce concept dans un contexte de médias sociaux, compte tenu de la vitesse à laquelle leurs services changent.

Alors je crois que nous avons cela dans une certaine mesure. Je crois que nous aurions simplement besoin de le renforcer un peu pour faire en sorte qu'il soit mieux mis en place.

M. Brad Butt: Voyez-vous cela comme quelque chose que le Parlement, par l'intermédiaire d'une loi, de modifications à la LPRPDE ou d'une autre façon...? Avons-nous besoin d'une loi canadienne pour garantir ce principe ou, selon vous, c'est quelque chose que l'industrie pourrait faire en exerçant des pressions morales, par exemple?

M. Tamir Israel: Je crois que c'est une combinaison des deux. Le principe doit être en place sous le régime de la LPRPDE, et je suis d'accord avec M. Kardash que cette loi a vraiment permis de mettre en place un cadre de principe très large que la commissaire à la protection de la vie privée a appliqué avec souplesse, comme une coréglementation, en ce sens que les lignes directrices sont publiées et les entreprises tentent de les suivre, et on discute avec l'industrie, et parfois avec d'autres intervenants, de la façon de les élaborer et de les appliquer.

Je crois que c'est le mécanisme qui convient, mais le principe même doit être intégré à la loi, et ensuite il faut qu'il y ait la possibilité, au moins, d'imposer une amende dans les cas de non-conformité grave, les cas de non-conformité flagrante, mais pas les cas limites ou quelque chose du genre. Ensuite, dans ce contexte, je crois que vous pouvez élaborer un cadre de coréglementation dans lequel les principes sont appliqués avec souplesse. Je crois que c'est la façon de procéder.

M. Brad Butt: Est-ce que les autres témoins aimeraient formuler des commentaires à cet égard avant que je passe à l'autoréglementation...?

M. Adam Kardash: C'est une excellente question. Dans les forums et les groupes de réflexion internationaux qui discutent des questions de protection de la vie privée, une des questions émergentes porte entièrement sur le consentement. En fait, la question n'est pas de savoir s'il devrait s'agir d'un consentement exprès ou facultatif, comme vous le mentionniez, ou d'un formulaire de retrait du consentement; elle est plutôt posée dans un contexte de protection efficace de la vie privée. Le consentement est-il même la solution? Peut-être que c'est une façon d'exercer un contrôle musclé sur les utilisateurs, comme l'a mentionné votre collègue, M. Calkins, dans le contexte d'une gouvernance de la vie privée vaste et holistique. Pour savoir ce que cela signifie exactement, je vous invite une fois de plus à consulter l'excellent manuel d'orientation conjoint publié par les autorités de réglementation en matière de protection de la vie privée. Il est très exhaustif et contient plus d'une centaine d'attentes quant à la façon d'offrir des protections appropriées en matière de vie privée d'une manière qui soit équilibrée pour les entreprises.

La question est de savoir si, une fois que vous vous concentrez seulement sur le consentement comme élément déclencheur pour entrer dans un site ou utiliser une technologie orientée strictement vers l'utilisateur, il devient rapidement inutile en lui-même pour vraiment rehausser les protections en matière de vie privée, car une fois que vous l'obtenez, vous devez toujours traiter de façon plus radicale les préoccupations plus vastes, et elles deviennent plus importantes.

Voilà pourquoi à l'échelle internationale, on a tendance à accorder une importance moindre au consentement, comme le font bien des cadres législatifs en vigueur.

● (1220)

M. Brad Butt: Monsieur Grimes, vouliez-vous dire quelque chose? Pas à ce sujet?

Ai-je terminé?

[*Français*]

Le président: Oui, le temps est écoulé.

M. Brad Butt: Merci beaucoup.

Le président: Je donne la parole à M. Boulerice, pour cinq minutes.

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

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

Pour commencer, je veux poser une question de base aux trois témoins. Si j'ai bien compris, le modèle d'affaires des réseaux sociaux est basé sur la collecte d'informations personnelles, qu'ils vendent ensuite à des compagnies qui ciblent ces gens pour leur vendre des produits.

Si on essaie de protéger la vie privée des gens et les renseignements personnels de ceux qui utilisent les médias sociaux, ne va-t-on pas contre la nature même du système, qui consiste à recueillir des informations et à les vendre ensuite à des compagnies qui ont intérêt à les avoir?

[*Traduction*]

Mme Sara Grimes: Je suppose que cela dépend de votre façon de définir les médias sociaux — si vous pensez exclusivement à Facebook comme média social, c'est le modèle commercial et c'est comme cela qu'il fonctionne. J'utilise une définition plus large, car les types de médias sociaux que les enfants utilisent comprennent des jeux et toutes sortes de choses différentes.

Bien des jeux en ligne qui fonctionnent auprès des enfants sont des modèles auxquels il faut s'abonner. Ils paient un forfait mensuel. Il n'y a pas de vraie raison pour procéder à un forage supplémentaire des données. Cela rapporte plus d'argent, je suppose, et donne une meilleure vision du marché, mais une grande partie de cela pourrait probablement être fait — je parle de la vision du marché — avec la permission et le consentement de l'utilisateur et dans le cadre d'un processus plus transparent.

Prenez par exemple le Club Penguin. Il appartient à Disney. C'était une entreprise canadienne, et il existe toujours des liens à l'entreprise canadienne qui l'a fondé. C'est un modèle auquel il faut s'abonner. Les enfants paient un forfait mensuel nominal pour y jouer. C'est un jeu extrêmement populaire. Ils ne font pas de publicité à titre de tiers, alors il n'y a pas ce lien explicite, et ils font eux-mêmes tout leur forage de données. Nous ne savons pas ce que cela peut être, mais il n'est pas du tout vrai qu'ils ont entièrement besoin de faire du forage et de la vente de données pour fonctionner. Ils ont des dizaines de millions de joueurs qui paient chaque mois pour pouvoir jouer.

Je crois que cela dépendrait de la définition.

M. Tamir Israel: Pour être bien clair, Facebook ne vend pas de données à des courtiers en information. Il utilise en fait le même type de modèle. Il s'agit d'un modèle de commercialisation interne dans lequel l'information ne sort pas. Si j'étais publicitaire, je choisirais les cinq catégories de gens auxquels je voudrais montrer mes publicités. Il est donc très efficace à cet égard.

Selon la conclusion à laquelle est arrivée notre commissaire à la protection de la vie privée sur les pratiques de Facebook, il peut y avoir certains types de publicité ciblée inhérente à son modèle d'affaires, publicité qui est acceptable et que tout le monde comprend. La question est de savoir jusqu'où l'on peut aller et lorsqu'il s'agit de types de données de nature plus délicate, de quelle façon cela est contrôlé.

Quant aux autres types de courtiers en information, ce sont des gens avec lesquels je n'ai jamais traité ni eu aucun contact d'ailleurs. Ils recueillent des données qui sont déjà publiques ou utilisent d'autres moyens dont je ne me sers pas nécessairement et que je trouve un peu plus discutables.

Je pense qu'il y a donc des niveaux différents de modèles d'affaires et qu'il faut adopter des approches souples face à chacun d'entre eux, mais je crois que, de façon générale, il y a de la place pour de l'amélioration.

M. Adam Kardash: Je n'ai rien d'autre à ajouter, sinon que les services sont gratuits. Ils sont donc appuyés, comme en témoigne la décision du Commissariat à la protection de la vie privée concernant l'enquête sur Facebook, par certaines pratiques et on les a jugés conformes à la LPRPDE.

Quant aux pratiques plus générales auxquelles vous faites allusion touchant les données associées à la publicité, le Commissariat à la protection de la vie privée du Canada a fait de nouveau preuve de leadership en proposant des lignes directrices sur la publicité axée sur les comportements en ligne. Ces lignes directrices seront combinées au cadre volontaire mis au point par l'industrie pour permettre aux particuliers de faire des choix dans ce contexte.

● (1225)

[*Français*]

M. Alexandre Boulerice: Ma prochaine question s'adresse à M. Israel. Elle porte sur Acxiom, ou les courtiers en données en ligne. C'est la première fois que j'en entends parler. Je trouve que c'est un peu inquiétant.

Y a-t-il plusieurs de ces joueurs? Comment recueillent-ils leurs informations et leurs données, et à qui les vendent-ils?

[*Traduction*]

M. Tamir Israel: Désolé, pourriez-vous répéter, s'il vous plaît.

[*Français*]

M. Alexandre Boulerice: J'aimerais savoir qui sont ces joueurs. Y en a-t-il plusieurs? Où prennent-ils leurs informations et à qui les vendent-ils?

[*Traduction*]

M. Tamir Israel: Moi aussi, j'aimerais le savoir.

Il y en a un certain nombre. Je crois qu'Acxiom est l'un des grands protagonistes, mais il y en a d'autres. Je pense à ChoicePoint, par exemple, dont le cas est intéressant. Cette société recueille des données de diverses sources et crée des profils dont on se sert aux fins d'application de la loi aux États-Unis.

Il y en a donc un certain nombre, et de taille variée, d'où la difficulté d'avoir un tableau complet de ce secteur et de savoir exactement comment les données circulent. Certaines données proviennent des immenses quantités d'informations qui sont publiques. Dans le contexte des médias sociaux, ce serait donc l'un des facteurs à prendre en compte lorsque l'on décide de choisir les paramètres par défaut pour la protection des renseignements personnels et d'autres données de ce genre.

Quant à la possibilité que les informations que contiennent ces bases de données proviennent de sites comme Facebook ou autres — et je ne veux pas faire ici de distinction entre ces sites —, il y a bien d'autres applications tierces qui sont intégrées à Facebook, telles que FarmVille et autres jeux de ce genre.

Je crois qu'aux termes de ses conditions d'utilisation, Facebook interdit la vente d'information à des courtiers, mais on ne sait pas exactement comment cette règle est appliquée. Techniquement, Acxiom pourrait créer sa propre application et la mettre sur Facebook.

[*Français*]

Le président: Merci.

[*Traduction*]

M. Adam Kardash: Il est important de souligner que les entreprises dont on a parlé sont américaines et l'on ne sait pas dans quelle mesure elles pourraient même opérer au Canada. Si elles le faisaient, elles seraient soumises à toute une série d'exigences qui leur interdiraient de mener des activités autorisées aux États-Unis.

Il ne faut donc pas oublier que les entreprises qui mènent ce genre d'activités n'ont pas leur siège au Canada. Les entreprises que nous avons mentionnées sont américaines.

[*Français*]

Le président: Malheureusement, votre période de temps écoulée.

Je cède les cinq dernières minutes d'aujourd'hui à M. Dreeshen.

[*Traduction*]

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

Et merci aux témoins d'être venus; vos commentaires sont très intéressants.

M. Boulerice vient de parler d'un sujet sur lequel j'essayais de me faire une idée précise, à savoir, qui sont ces courtiers en information et comment gagnent-ils leur vie? Je suppose qu'en tant que comité, c'est un sujet que nous pourrions fouiller et si vous avez d'autres informations à ce sujet, nous voudrions certainement l'avoir.

Monsieur Kardash, vous avez parlé de la documentation de l'Alberta et de la Colombie-Britannique et des attentes de ces deux provinces dans ce domaine. Je suis sûr que le comité aimerait bien obtenir cette information pour pouvoir l'étudier.

Parmi les quatre autres points que vous avez soulevés, monsieur Kardash, vous avez parlé des répercussions que les changements pourraient avoir sur la Constitution et sur lesquels il faudrait réfléchir. Pourriez-vous élaborer à ce sujet?

M. Adam Kardash: D'accord.

La LPRPDE est fondée sur le pouvoir constitutionnel accordé aux termes du second élément du pouvoir fédéral de réglementation des échanges et du commerce. Lorsqu'elle est entrée en vigueur pour la première fois, on s'est d'ailleurs interrogé sur sa validité constitutionnelle. Pour des raisons que j'ignore, le sujet a été abandonné.

Tout récemment, la Cour suprême du Canada a rendu un verdict par rapport au poste d'administrateur national des valeurs mobilières et à la volonté de créer un tel poste. Dans ce contexte, elle a déclaré à l'unanimité qu'il serait inconstitutionnel d'invoquer le pouvoir fédéral de réglementation des échanges et du commerce.

Cela nous a amenés, surtout nous qui travaillons dans le domaine de la protection des renseignements personnels, à nous interroger sur la pertinence de ce jugement pour la LPRPDE, notamment dans le contexte d'un éventuel accroissement des pouvoirs d'application de la loi accordés au Commissariat à la protection des renseignements personnels du Canada.

C'est aux experts constitutionnels d'en décider et je n'en suis pas. Mais cet important verdict de la Cour suprême du Canada mérite, à mon avis, d'être étudié par rapport à toute initiative législative que l'on pourrait prendre, surtout si elle devait élargir les pouvoirs d'application de la loi.

● (1230)

M. Earl Dreeshen: Merci.

Madame Grimes, vous avez passé en revue quatre différents thèmes, à savoir la réglementation des données propres aux enfants, un libellé plus précis du consentement libre et éclairé et, si je ne m'abuse, la liberté d'expression des droits, de même que le leadership et l'application de la loi.

Vous avez aussi parlé de certaines entreprises canadiennes qui ont élaboré des pratiques vraiment exemplaires. Pourriez-vous élaborer un peu à ce sujet?

Mme Sara Grimes: Oui, je suis vraiment contente que vous me posiez la question, parce que j'aime beaucoup parler de ces bons exemples, par opposition à certaines pratiques effrayantes et extrêmes que l'on peut voir.

L'une des entreprises canadiennes de médias sociaux exemplaires est Storybird, dont le siège est à Ottawa, mais qui a aussi un bureau, je crois, à Toronto. Sa politique de protection des renseignements personnels est rédigée pour les enfants et les parents. Elle explique toutes sortes de choses, et même des choses que l'entreprise ne fait pas — comme la collecte de données qui est pratiquée sur d'autres sites — comme façon de se démarquer. Storybird est un site de médias sociaux qui permet aux enfants, aux parents et aux enseignants de créer des livres d'images et de les échanger. Ce site très dynamique est aussi utilisé dans les écoles. Cela fait donc plaisir de voir ainsi largement diffusées d'excellentes politiques de protection des renseignements personnels.

Je pense aussi à Frima Studio, qui a son siège à Montréal et qui crée des jeux en ligne. J'ai suivi la compagnie pendant les années qu'elle a consacrées à élaborer une politique de protection des renseignements personnels dans une langue que puissent comprendre les enfants, mais bien articulée et mettant à leur portée des concepts juridiques très complexes. Elle aussi a expliqué les choses qu'elle ne faisait pas, et celles qu'elle faisait.

Comme dernier exemple, je pense à zinc Roe, une entreprise torontoise qui crée des applications. Elle a été l'une des premières à consulter des universitaires, des défenseurs des droits des enfants et des parents pour protéger et traiter l'information que les tout-petits créent et partagent, et celle que les parents créent à leur sujet. C'est un domaine très sensible. L'entreprise a donc vraiment cherché à trouver des pratiques exemplaires en matière de déontologie.

Ce sont là trois exemples d'entreprises que j'aimerais voir participer davantage à ces débats, car elles ont d'excellentes idées qu'elles ont su mettre en pratique.

M. Earl Dreeshen: Merci.

[*Français*]

Le président: Votre temps est écoulé. C'est ce qui conclut le témoignage des trois invités d'aujourd'hui. Je vous remercie de votre présence.

Je suspends la séance pour quelques minutes, et nous reviendrons ensuite pour discuter des travaux futurs du comité.

● _____ (Pause) _____

●

● (1235)

Le président: Nous abordons maintenant le deuxième point à l'ordre du jour.

Monsieur Warkentin, voulez-vous dire quelque chose?

[*Traduction*]

M. Chris Warkentin (Peace River, PCC): Merci, monsieur le président.

Je proposerais que nous passions à huis clos pour traiter des travaux du comité.

[*Français*]

Le président: M. Warkentin a présenté une motion pour poursuivre la séance à huis clos. Comme elle ne peut pas faire l'objet d'un débat, il y aura un vote par appel nominal.

(La motion est adoptée par 7 voix contre 4.)

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