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 051 • 1re SESSION • 41e LÉGISLATURE

**TÉMOIGNAGES**

## Le jeudi 18 octobre 2012

---

## Président

**M. Pierre-Luc Dusseault**

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

**Le jeudi 18 octobre 2012**

● (1530)

[*Français*]

**Le président (M. Pierre-Luc Dusseault (Sherbrooke, NPD)):** Bonjour à tous.

Monsieur Lawford, je vous remercie de votre présence. Vous êtes notre seul témoin aujourd'hui.

Comme prévu à l'ordre du jour, on consacrera environ une heure aux témoignages et aux questions. On va commencer par une présentation de 10 minutes. Par la suite, les membres pourront poser des questions, comme d'habitude. Finalement, pendant la deuxième heure, on siégera à huis clos, pour un compte rendu des séances de travail à l'étranger.

Je vais tout de suite laisser la parole à M. Lawford pour 10 minutes.

**M. John Lawford (directeur exécutif et avocat général, Centre pour la défense de l'intérêt public):** Merci, monsieur le président.

[*Traduction*]

Je suis seul aujourd'hui. Mme Janet Lo, ma collègue, a dû s'excuser. Elle est en séance à huis clos au CRTC sur le dossier de Bell-Astral.

Le Centre pour la défense de l'intérêt public est une organisation à but non lucratif qui offre des services juridiques et de recherche pour le compte du consommateur, notamment le consommateur vulnérable, en ce qui concerne l'offre de services publics importants. Nous avons beaucoup travaillé avec la Loi sur la protection des renseignements personnels et les documents électroniques depuis son adoption, et ce du point de vue du consommateur. Nous avons publié quelques rapports récemment qui portent sur la protection des renseignements personnels des enfants en ligne, la création d'une liste d'interdiction de suivi des télécommunications et les atteintes à la protection des données.

J'ai remis au greffier des exemplaires des rapports ainsi que des résumés.

Nous sommes ici aujourd'hui pour discuter de la protection des renseignements personnels à court terme, ce qui sera largement définie par des services comme les réseaux sociaux. Cependant, les réseaux sociaux posent des défis en ce qui concerne les renseignements personnels et les intérêts commerciaux qui y sont liés.

Notre centre a déposé une plainte récemment auprès du Commissariat à la protection de la vie privée du Canada en vertu de la Loi sur la protection des renseignements personnels et les documents électroniques. La plainte visait Nexopia.com Inc., un réseau social dont le siège est en Alberta et qui vise essentiellement un public adolescent. Cet exemple réel montre bien les défis qui sont liés à la vie privée et aux réseaux sociaux et malheureusement, les lacunes de la Loi sur la protection des renseignements personnels en ce qui concerne des pratiques douteuses d'atteinte à la vie privée, même celle des enfants et des adolescents.

Notre centre affirme que Nexopia n'aurait fourni aucune description compréhensible de la collecte, de l'utilisation et de la divulgation de renseignements personnels recueillis aux utilisateurs, essentiellement mineurs, de son site. Nous avons indiqué que la société n'aurait pas suffisamment décrit ses pratiques en matière de divulgation de renseignements aux annonceurs, ni son utilisation des renseignements pour concevoir des annonces ciblant des adolescents. Nous nous sommes plaints du fait que les réglages par défaut concernant les renseignements personnels comme le sexe, l'âge, la localité et des images étaient disponibles sur Internet et n'étaient même pas restreints aux membres du site. Nous avions comme prémisse que ce n'était pas raisonnable et que c'était même dangereux pour les jeunes utilisateurs du site. Nous avons conclu en indiquant que Nexopia semblait conserver les données personnelles pour une période illimitée, même après la suppression d'un compte.

La Commissaire à la protection de la vie privée nous a donné gain de cause sur toutes nos allégations. C'était en février 2012, deux années après le dépôt de notre plainte.

En ce qui concerne les réglages par défaut, je citerai la Commissaire à la protection de la vie privée:

> Nous considérons que les attentes raisonnables des utilisateurs, surtout ceux qui ont clairement indiqué qu'ils préféreraient échanger moins de renseignements, ne sont pas respectées quand on rend une partie du profil accessible à quiconque sur Internet.

Et pourtant, Nexopia a indiqué à la Commissaire à la protection de la vie privée qu'elle ne suivrait pas les quatre recommandations portant sur la conservation des données. La Commissaire a dû faire appel à la Cour fédérale pour rendre exécutoire sa décision. Pourquoi?

Tout d'abord, la Commissaire à la protection de la vie privée ne peut rendre des ordonnances, ni imposer des amendes. Si les décisions en matière de protection des renseignements personnels coûtent trop cher aux réseaux sociaux ou leur causent trop d'inconvénients, ces réseaux peuvent, semble-t-il, continuer à violer la vie privée des gens.

Deuxièmement, ce refus révèle la vraie nature des réseaux sociaux: ils sont financés par les renseignements personnels. Leur demander de détruire des données, c'est leur demander de se priver d'un bien.

La requête de la Commissaire à la protection de la vie privée auprès de la Cour fédérale montrera bien si ce sont les intérêts commerciaux ou la protection de la vie privée des particuliers qui priment en vertu de la Loi sur la protection des renseignements personnels et les documents électroniques. Cependant, les membres de votre comité sont confrontés à une question plus élargie, c'est-à-dire comment concevoir des lois qui permettent d'éviter ce type de conflit, notamment dans le domaine du réseautage social et de la vie en ligne, domaine qui évolue rapidement.

Je vais maintenant parler du projet de loi C-12 et de la notification des atteintes à la protection des données.

LinkedIn et eHarmony ont subi des vols importants de données ce printemps. Les réseaux sociaux sont maintenant de grandes cibles pour les pirateurs, et il y a donc le risque que soient divulgués des renseignements personnels recueillis sur ces sites qui ne sont pas destinés au grand public. Ces atteintes s'ajoutent aux fuites de renseignements personnels de sites relevées par la Commissaire à la protection de la vie privée dans son étude publiée à la fin septembre.

Le projet de loi C-12 vise à modifier la Loi sur la protection des renseignements personnels et les documents électroniques afin d'inclure une clause concernant la notification des atteintes à la protection des données. Malheureusement, cet objectif n'est pas réalisé. Les modifications permettraient à une société victime d'une atteinte de décider si l'atteinte est suffisamment importante pour être notifiée à la Commissaire à la protection de la vie privée. Pour ce faire, c'est encore la société qui effectue une évaluation en vue de déterminer si la cause de l'atteinte ou d'une série d'atteintes constitue un problème systématique.

● (1535)

À notre avis, il est fort peu probable qu'une société, et surtout un réseau social qui vend des données, ne déclare qu'elle a un problème systématique d'atteinte à la protection des données et des procédures de traitement de données qui donnent lieu à des fuites.

Le projet de loi C-12 demande aux sociétés de déclarer qu'elles sont en fait négligentes. Par conséquent, nous prédisons avec confiance qu'en vertu du projet de loi C-12, un réseau ou une autre société en ligne n'informera presque jamais la Commissaire à la protection de la vie privée d'une atteinte qui n'a pas été rendue publique autrement. Aux termes du projet de loi, ce serait les sociétés qui décideraient s'il y a lieu de signaler directement aux consommateurs les atteintes à la protection des données. Ce sont les sociétés qui devront décider s'il est raisonnable, compte tenu des circonstances, de croire que l'atteinte créée un risque réel de préjudice pour la personne concernée.

Tout d'abord, ce seuil est très élevé. C'est encore plus élevé que ne le prévoit la législation des États-Unis et ce n'est pas réaliste. Il est difficile de prédire les usages abusifs des renseignements personnels.

Deuxièmement, le projet de loi C-12 fait fi des motivations plus qu'évidentes des sociétés, qui ne constateront aucun risque à l'égard des particuliers et éviteront de notifier la commissaire de ces atteintes et ainsi les coûts afférents. Par conséquent, nous vous affirmons qu'en vertu du projet de loi C-12, les réseaux sociaux et les autres sociétés en ligne ne signaleront presque jamais aux particuliers une atteinte qui n'a pas été rendue publique par un autre moyen.

Au Canada, il existe un autre modèle pour les textes législatifs portant sur les atteintes à la protection des données, et c'est la loi de l'Alberta sur la protection des informations personnelles. En Alberta, toute atteinte doit être signalée au commissaire à la protection de la vie privée de cette province, sous peine d'amende. Le commissaire décide ensuite si l'atteinte mérite d'être signalée aux particuliers en évaluant le risque de préjudice.

Notre centre a sondé l'opinion publique à l'égard de la notification d'atteintes à la protection des données en 2011 en soumettant la question à des groupes de discussion. La vaste majorité des participants ont préféré le modèle établi par l'Alberta, plutôt que de confier la décision aux sociétés. Nous recommandons au comité d'exprimer ces préoccupations concernant la notification des atteintes à la protection des données dans son rapport sur le projet de loi C-12.

Je vais maintenant vous parler des politiques en matière de protection des renseignements personnels. Les politiques de protection des renseignements personnels des réseaux sociaux exigent une adhésion totale. C'est l'utilisateur qui assume le risque en ce qui concerne les renseignements personnels. Et pourtant, les réseaux sociaux misent sur le consentement des utilisateurs pour justifier leurs pratiques et indiquent que l'utilisation d'un site constitue un consentement à leur politique de protection des renseignements personnels.

Selon le Centre pour la défense de l'intérêt public, cette fiction juridique remplace le consentement éclairé sur bon nombre de réseaux sociaux. Les utilisateurs ne lisent pas tout le texte de la politique et même s'ils le font, ils ne la comprennent pas. Pourquoi? C'est parce que les grands réseaux sociaux définissent les « renseignements personnels » d'une façon qui prête à confusion, et aucune des définitions ne correspond à celle prévue dans la Loi sur la protection des renseignements personnels et les documents électroniques.

De nombreux sites définissent les renseignements personnels comme étant des informations personnellement identifiables, ce qui est, comme vous le savez, un concept issu du droit américain. Plus récemment, un certain nombre des grands sites ont retiré leur définition des renseignements personnels et ne donnent que des exemples du traitement de certaines données comme le sexe ou l'âge. Vous devriez disposer d'une copie d'un document que j'ai remis au greffier qui contient des exemples de politiques en matière de protection de la vie privée dont je vous ai parlé.

Cette non-définition de renseignements personnels est importante, car les utilisateurs qui lisent une politique en la matière ne sont pas en mesure de comprendre véritablement leurs droits en vertu de la Loi sur la protection des renseignements personnels afin de déposer une plainte, d'exiger le respect de la loi ou même de contacter la société.

La Commissaire à la protection de la vie privée a comparu devant votre comité et a indiqué que les sites de réseautage social n'expliquent pas suffisamment comment ils utilisent les renseignements personnels. Elle doute que dans de telles situations, un site de réseautage social dispose d'un consentement réel. Nous sommes du même avis que la commissaire. Cependant, le mécanisme de dépôt de plainte prévu par la loi n'a pas de mordant. La commissaire doit être habilitée à rendre des ordonnances et à imposer des amendes.

Notre centre propose donc, vu les défis associés à la collecte à grande échelle de données par les sociétés de réseautage social et autres en ligne, que le comité aille plus loin et songe à des mesures exécutoires d'application de la loi telles que celles qui existent dans le cas des agences de télémarketing qui ne respectent pas la liste d'exclusion des appels et violent ainsi la loi canadienne en matière de protection de la vie privée.

En guise de conclusion, je vous ferai part de certaines idées novatrices concernant le réseautage social et la protection de la vie privée.

Tout d'abord, il existe de nombreuses entités qui traitent les données personnelles recueillies sur les sites de réseautage social afin d'en réaliser un profit au moyen de publicités et d'autres méthodes. Le comité devrait étudier les rapports entre ces intervenants et songer à des règles qui exigeraient la divulgation des parties ayant des liens dans le commerce de données personnelles comme celles qui existent pour les valeurs mobilières, et ce, afin d'accroître la transparence de l'échange de données entre les sites de réseautage social et les agences de marketing.

Deuxièmement, le comité devait se pencher sur une éventuelle liste nationale d'interdiction du suivi des télécommunications.

Troisièmement, le comité devrait étudier les liens entre le droit de la protection de la vie privée et le droit de la concurrence, afin de déterminer si le Bureau de la concurrence devrait occuper un rôle dans la protection de la vie privée et si une fusion ou une autre pratique commerciale pourrait nuire à la concurrence. Sur de nombreux marchés en ligne, la compétition que se livrent les commerçants pour les visiteurs dépend de la nature des renseignements personnels ou de la valeur des grandes bases de données.

● (1540)

Le Centre pour la défense de l'intérêt public vous remercie de lui avoir accordé cette occasion de témoigner. Nous nous ferons un plaisir de répondre à vos questions.

[*Français*]

et en anglais et en français.

Merci.

**Le président:** Merci de cette excellente présentation, monsieur Lawford.

On va passer à la période de questions et réponses de sept minutes, en commençant par M. Angus.

[*Traduction*]

**M. Charlie Angus (Timmins—Baie James, NPD):** Merci, monsieur le président.

Et merci à vous, monsieur. Vos propos sont fort intéressants. Si vous avez suivi notre étude sur la question des médias sociaux, vous saurez que nous sommes aux prises avec deux grandes priorités. L'une, le fait de ne pas entraver le développement, et l'autre, de s'assurer que nos citoyens les plus vulnérables, notamment les jeunes, ne sont pas ciblés de façon démesurée, et que la vie privée des gens est protégée comme il se doit.

Certains des grands pilotes sur cette nouvelle autoroute de l'information nous ont indiqué qu'ils ne font jamais d'excès de vitesse, qu'ils s'arrêtent toujours aux feux rouges, qu'ils ne font jamais de manoeuvres illégales, qu'il ne faut pas avoir de police sur cette autoroute des données et que tout ira bien.

Je suis préoccupé par Nexopia, qui n'a pas respecté la décision de la commissaire à la protection de la vie privée... Il me semble que la commissaire a souligné 24 manquements dans le traitement des informations par Nexopia. La société n'a pas respecté les délais imposés par la commissaire et conteste même certaines de ses recommandations devant la cour.

Croyez-vous que la commissaire devrait avoir davantage d'outils afin d'assurer le respect de ses décisions et l'observation des règles par tous les joueurs présents sur le marché?

**M. John Lawford:** Oui, et la plainte déposée contre Nexopia en est un bon exemple. On aurait pu également choisir d'autres sites de réseautage social. Nous avons ciblé un site qui ne semble pas avoir indiqué clairement à ses utilisateurs l'usage qui serait fait des renseignements recueillis. La commissaire nous a donné gain de cause et la société n'a pas respecté la décision. Il se peut qu'au final Nexopia obtempère, mais c'est une façon très inefficace de procéder, alors qu'en Alberta, en Colombie-Britannique et au Québec, les commissaires à la protection de la vie privée peuvent tout simplement rendre une ordonnance.

Il aurait été beaucoup plus sensé et direct si la commissaire avait rendu une ordonnance en février sans avoir à attendre pour voir si la société allait obtempérer. Selon la commissaire, la société est loin de respecter les exigences de la décision.

**M. Charlie Angus:** Nous ne cherchons pas à atteindre la réputation de Nexopia, mais leur modèle d'entreprise vise les jeunes gens, et les jeunes gens qui se servent d'Internet devraient se sentir libres, devraient avoir l'impression que lorsqu'ils utilisent un site, c'est pour parler avec leurs amis et ne pas être confrontés à des trolls. Et pourtant, vous semblez nous dire que le modèle d'entreprise de Nexopia, c'est que n'importe qui peut suivre les utilisateurs du site et connaître leur sexe, leurs préférences ainsi que leur école. L'orientation sexuelle ou encore d'autres facteurs sont-ils affichés sur le site? Est-ce le type de renseignements que peut trouver n'importe qui?

**M. John Lawford:** Voilà la raison d'être de notre plainte. Nous avons déposé cette plainte parce que n'importe qui peut aller sur Nexopia, qui fournit même un outil de recherche fort convivial pour les utilisateurs non inscrits, afin de trouver, dès la page d'accueil, l'âge, le sexe et la localité de l'utilisateur. Une fois ces données obtenues, la personne peut choisir des intérêts et cibler certaines personnes afin d'en dresser des profils. Il donc possible d'obtenir des profils réels sans être membre du réseau.

Ce site est également indexé sur Google et d'autres moteurs de recherche, ce qui veut dire que l'on a juste à taper « sexe féminin, 13, Calgary, danse » suivi de « :nexopia.com » afin de trouver des profils de cette source. Nous sommes d'avis que ce n'est pas exactement...

Cela ne correspond pas aux attentes de la gamine de 13 ans qui s'inscrit. Elle s'attend à partager des renseignements avec ses amis et non pas à être connue de tous les utilisateurs d'Internet.

● (1545)

**M. Charlie Angus:** C'est ce qu'a conclu la commissaire à la protection de la vie privée. Elle a indiqué que les règles ne répondaient pas aux normes concernant la protection d'une classe vulnérable de notre société. La société Nexopia a-t-elle changé les réglages par défaut?

**M. John Lawford:** La société a été priée de modifier sa politique en matière de protection des renseignements personnels et autres au plus tard le 30 juin, date limite qui n'a pas été respectée. La société devait modifier ses réglages par défaut au plus tard le 30 septembre, afin que les nouveaux membres s'inscrivent par défaut comme étant visibles uniquement à leurs amis, et ne puissent faire l'objet d'une recherche effectuée depuis l'extérieur du site. Cette date butoir n'a pas été respectée.

**M. Charlie Angus:** C'est inquiétant, parce que je sais que la Commissaire à la protection de la vie privée a saisi la Cour fédérale concernant le refus de la société de supprimer des données. Nous avons tous été touchés par l'histoire terrible de Amanda Todd, qui a été la victime de cyber-intimidation, et nous avons tous lu son mot très touchant: « Je ne pourrai jamais récupérer la photo. Elle sera toujours là. »

Si un adolescent de 15 ans n'aime pas ce qui se passe sur Nexopia ou ne veut plus en faire partie et supprime son compte, les données seront toujours détenues par une société commerciale. Vous nous dites que Nexopia est prête à passer devant la cour afin de continuer à détenir ces données même si un jeune voudrait les faire supprimer?

**M. John Lawford:** Non, je vous dis que lorsque la Commissaire a demandé à Nexopia d'instaurer une politique sur la gestion des données et de fournir aux utilisateurs un véritable pouvoir de suppression des données, la société a refusé. La Commissaire, qui n'a aucun pouvoir exécutoire et ne peut qu'émettre des recommandations, a estimé que le principe était suffisamment important pour qu'elle saisisse la Cour fédérale afin de faire respecter sa décision .

**M. Charlie Angus:** Pouvez-vous nous expliquer pourquoi les jeunes personnes, ou encore toute personne qui décide de ne plus être membre d'un site, devrait avoir ce pouvoir de suppression des données? Peut-être que les choses deviennent un peu trop bizarres ou que ces jeunes veulent juste reprendre le contrôle de leur vie. Pourquoi cette possibilité devrait-elle être bien indiquée et disponible?

**M. John Lawford:** Nous croyons que les utilisateurs et les gens... C'est presque un droit essentiel. On devrait pouvoir demander à une société de supprimer des renseignements. La loi précise bien que les sociétés sont censées supprimer les données qui ne servent plus, donc nous ne comprenons pas pourquoi les utilisateurs ne devraient pas avoir un droit de suppression des données.

En Europe, les débats portent sur le choix entre le droit d'oublier et le droit de supprimer. Ce débat est naissant au Canada. Je crois qu'il devrait avoir lieu, car notre Centre est persuadé qu'il revient à l'utilisateur le droit d'effacer son compte.

**M. Charlie Angus:** Les sociétés créent des sites qui permettent aux jeunes gens d'échanger des renseignements et de faire toutes sortes de choses formidables, mais il faut imposer des règles de base afin que les mauvais éléments ne puissent pas profiter des jeunes.

Est-ce imposer une responsabilité démesurée lorsqu'on demande aux sociétés comme Nexopia d'établir des réglages par défaut qui protègent la vie privée ou de supprimer des comptes lorsque les utilisateurs le demandent?

**M. John Lawford:** La Commissaire à la protection de la vie privée a bien expliqué que c'est ce que précisent déjà les dispositions de la loi en vigueur.

Or, cela devient problématique lorsqu'une société dit: « C'est bien beau. Merci beaucoup. En dépit de votre décision, nous continuerons à faire ce que nous voulons. » Le problème, c'est l'exécution de la décision. Le comportement des sociétés est bien couvert par la loi. Nous avons eu gain de cause sur les 24 allégations de notre plainte. Je ne sais pas trop comment on pourrait améliorer la loi. On pourrait peut-être tenter de la rendre plus claire. Le comité pourrait se pencher sur la question. En ce qui concerne la conservation des données, par exemple, il n'est pas clair que c'est l'utilisateur qui a le droit de supprimer les données. On précise uniquement qu'il devrait y avoir des durées minimale et maximale de conservation. On pourrait peut-être rendre la disposition plus claire.

**M. Charlie Angus:** Merci beaucoup.

[*Français*]

**Le président:** Monsieur Angus, votre temps de parole est écoulé.

Je cède la parole à Mme Davidson, qui dispose de sept minutes.

[*Traduction*]

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

Et merci à vous, M. Lawford d'être venu cet après-midi. Vous nous transmettez des renseignements très intéressants.

J'aimerais continuer dans la même lignée que M. Angus. Vous avez indiqué qu'on pourrait modifier certains aspects de la loi. Vous avez parlé de la conservation des données. Y a-t-il d'autres modifications que vous souhaitiez voir apporter à la loi?

● (1550)

**M. John Lawford:** Il est intéressant de poursuivre un peu cette question aussi. Au cours de la réunion, nous n'avons pas beaucoup entendu parler — et j'ai été à l'écoute — de la dépersonnalisation des renseignements personnels. Selon la loi, c'est équivalent, c'est-à-dire que vous pouvez dépersonnaliser ou supprimer ces renseignements.

Nos recherches laissent croire que certaines données ne sont jamais tout à fait dépersonnalisées; souvent, on peut les repersonnaliser. Il s'agirait donc d'un rajustement. Nous ne devrions peut-être pas présumer que dépersonnaliser signifie supprimer. Ce sont peut-être deux choses différentes.

**Mme Patricia Davidson:** Je ne sais même pas ce que dépersonnaliser signifie. Par contre, nous savons tous ce que supprimer signifie.

S'agit-il d'une autre méthode pour supprimer, ou pour donner l'impression de supprimer des données?

**M. John Lawford:** Oui, c'est un modèle très pratique pour certaines utilisations commerciales. Vous pouvez regrouper ou dépersonnaliser les renseignements et ensuite les utiliser à d'autres fins, par exemple, recenser les visiteurs de votre site Web et leurs achats, informer les annonceurs et les consommateurs, et modifier votre site pour qu'il fonctionne bien. Ce ne sont que quelques-unes des utilisations du modèle.

Lorsqu'on utilise les renseignements liés à la santé à des fins secondaires, il faut veiller à ce qu'il soit impossible de faire le lien entre une personne et son dossier, même lorsqu'on élimine certains identificateurs. Il faut un certain savoir-faire pour y arriver.

Pour ce qui est des autres rajustements en ce qui concerne la loi, le mécanisme de consentement est la bonne façon de procéder. Le problème que nous avons eu avec Nexopia et dans notre document sur l'utilisation des réseaux sociaux par les jeunes, c'est que les enfants ne comprenaient pas dans quelle mesure leurs renseignements personnels seraient utilisés à d'autres fins une fois qu'ils les avaient fournis. Peut-on, ici ou ailleurs, parler de différents niveaux de consentement selon l'âge?

Aux États-Unis — et je pense que M. Elder vous l'a mentionné —, la loi interdit aux entreprises de recueillir des renseignements personnels auprès des jeunes de moins de 13 ans. À mon avis, c'est un très bon règlement. Toutefois, nous n'en avons pas encore parlé au Canada; il est toujours possible de recueillir des renseignements au sujet d'enfants de deux ans. Selon la commissaire à la protection de la vie privée, c'est probablement contre les règles, mais c'est possible.

**Mme Patricia Davidson:** En ce qui concerne les politiques de la protection de la vie privée, je pense que vous avez dit qu'il s'agissait d'un choix à prendre ou à laisser, sans consentement éclairé. Je pense que nous avons beaucoup parlé de la vie privée et des formulaires de consentement. En effet, personne — adolescents ou adultes — ne les lit; on se contente de se rendre au bout et de cliquer sur le bouton « J'accepte ».

À votre avis, existe-t-il une façon de les normaliser et de faire en sorte que les utilisateurs les comprennent?

**M. John Lawford:** Une des choses que j'ai mentionnées dans mon exposé, c'est que les entreprises définissent les renseignements personnels en fonction de l'utilisation qu'elles en feront. Même si cela peut être acceptable, il pourrait être pertinent d'ajouter un énoncé qui définit ce qu'est un renseignement personnel, conformément à la loi en vigueur à l'endroit où elles mènent leurs activités — par exemple, au Canada. De cette façon, l'utilisateur moyen pourrait faire des comparaisons. Je sais que c'est plus facile à dire qu'à faire, mais c'est certainement une possibilité.

Dans quelques documents, nous avons aussi parlé de la possibilité de concevoir des icônes faciles à comprendre ou des descriptions abrégées. Par exemple, dans le cas d'un site Web qui partage vos renseignements personnels, vous pourriez voir deux mains qui tendent un document, ou quelque chose du genre. À mon avis, cela aiderait les personnes pressées. C'est une option. Ce serait aussi certainement une très bonne idée de chercher à savoir s'il existe une façon de normaliser tout cela qui serait acceptée par tout le monde.

**Mme Patricia Davidson:** Comment appliquerait-on cela? En ferait-on une loi? Comment procéderait-on?

**M. John Lawford:** Il faudrait peut-être modifier la loi pour préciser qu'il faut utiliser la définition des renseignements personnels donnée dans la loi. Par ailleurs, je pense que la commissaire à la protection de la vie privée pourrait s'en occuper par l'entremise d'une table ronde avec les parties intéressées. Il pourrait s'agir de lignes directrices si cela venait des échelons plus élevés, mais cela se ferait probablement par l'entremise de la commissaire à la protection de la vie privée plutôt que par une loi, car à mon avis, il pourrait être trop difficile d'en faire une loi.

**Mme Patricia Davidson:** Étant donné que la technologie évolue beaucoup plus rapidement que la loi, est-il risqué de trop légiférer? Vaut-il mieux ne pas en faire une loi?

**M. John Lawford:** Prenons l'exemple des atteintes à la protection des données. On a démontré que, même avec la loi en vigueur, nous pouvions avoir à faire face au piratage informatique ou à des méthodes de gestion de données qui peuvent devenir un problème chronique. Il vaut la peine de modifier la loi en conséquence. Par ailleurs, la loi elle-même, c'est-à-dire la LPRPDE, reste neutre au sujet de la technologie et est rédigée en termes très généraux. Elle a seulement besoin de quelques rajustements. On ne doit pas lui apporter de grands changements, car elle offre déjà un bon cadre. À notre avis, elle a seulement besoin d'être appliquée plus sévèrement.

● (1555)

**Mme Patricia Davidson:** J'aimerais revenir un moment à la question de Nexopia et des 24 préoccupations qui ont été soulevées. Je pense que l'entreprise a accepté de se conformer à 20 d'entre elles, mais elle a refusé de le faire pour les quatre autres.

**M. John Lawford:** C'est exact.

**Mme Patricia Davidson:** Ces quatre recommandations concernaient-elles des questions de conservation des données, ou s'agissait-il d'autre chose?

**M. John Lawford:** Elles concernaient toutes des questions de conservation.

**Mme Patricia Davidson:** Pourquoi seraient-elles différentes des autres? Pourquoi quatre d'entre elles seraient-elles différentes?

**M. John Lawford:** Je crois que l'une d'entre elles concernait le refus d'établir une période de conservation pour les nouveaux utilisateurs. Elle préciserait donc qu'il faut garder les données pendant trois ans après la fermeture du compte de l'utilisateur. Une autre option consistait à offrir un véritable bouton « Supprimer ». Il y en avait deux autres, mais je crois que je devrai consulter mon téléphone intelligent pour les trouver.

**Mme Patricia Davidson:** Existe-t-il un véritable bouton « Supprimer »?

**M. John Lawford:** Non. En ce moment, Nexopia va interrompre un compte de façon à ce qu'on ne puisse plus y avoir accès, mais il existe toujours dans leurs serveurs.

**Mme Patricia Davidson:** D'autres entreprises offrent-elles un véritable bouton « Supprimer »?

**M. John Lawford:** Les entreprises qui suppriment réellement des données sont peu nombreuses. D'après ce que je comprends, vous pouvez supprimer des éléments individuels dans Facebook. Mais il s'agit de savoir si ces éléments sont vraiment supprimés ou s'ils font l'objet d'une série de procédures de secours. On dit qu'ils sont réellement supprimés. Mais il faut y aller un par un; vous ne pouvez pas facilement supprimer tout un profil. Je ne connais aucun site Web qui s'en tire bien sur ce plan en ce moment, mais je ne les connais pas tous.

**Mme Patricia Davidson:** Merci beaucoup.

[*Français*]

**Le président:** Votre temps de parole est écoulé.

Je cède la parole à M. MacAulay, qui s'est joint à nous aujourd'hui.

Vous disposez de sept minutes.

[*Traduction*]

**L'hon. Lawrence MacAulay (Cardigan, Lib.):** Merci, monsieur le président.

Je suis un nouveau membre du comité. J'ai aimé votre exposé et je vous suis reconnaissant d'être ici.

Même si Nexopia ne l'offre pas, existe-t-il un véritable bouton « Supprimer »? Y a-t-il un moyen de savoir que les données supprimées n'existent plus?

**M. John Lawford:** Je pense que c'est très difficile pour les réseaux sociaux, car ils sont conçus pour demander et ensuite conserver des renseignements. C'est la façon dont ils fonctionnent. Je ne crois pas qu'ils aient été conçus pour supprimer facilement les données de façon permanente et pour garantir et vérifier que cela a été fait, alors qu'un hôpital ou un autre système qui possède un meilleur service de gestion des données pourrait être en mesure de le faire.

Le problème souvent soulevé par les entreprises, c'est qu'elles font des sauvegardes, où les renseignements sont conservés. Une procédure de sauvegarde précédente les a aussi conservés, et vous ne pouvez jamais les supprimer. Donc, en théorie, on peut toujours y avoir accès.

Mais il s'agit simplement d'un élément de la conception du système. Si on les y obligeait, je suis certain que les entreprises seraient en mesure de l'intégrer dans leur prochaine version du système.

**L'hon. Lawrence MacAulay:** Encore une fois, c'est peut-être inapproprié, mais cela pourrait-il être fait? Il s'agit seulement d'une question d'opinion. Je pense que le bouton « Supprimer » pourrait se comparer à une conversation officieuse avec un journaliste: les renseignements communiqués resteront officieux jusqu'à ce que le journaliste en ait besoin. C'est essentiellement ce que vous êtes en train de nous dire.

**M. John Lawford:** En ce moment, je pense que c'est la réalité de la plupart des réseaux sociaux, car ils doivent conserver les données ou au moins les dépersonnaliser, afin qu'elles puissent être utilisées pour d'autres fins et ne pas perdre leur valeur.

**L'hon. Lawrence MacAulay:** À mon avis, c'est certainement grave lorsqu'on peut recueillir des renseignements sur leur sexe, leurs souhaits et ce genre de choses. C'est grave. Les entreprises font de l'argent grâce à ce genre de pratiques. C'est tout à fait inacceptable.

**M. John Lawford:** La commissaire à la protection de la vie privée a conclu qu'une grande partie de ces renseignements étaient sensibles, surtout en ce qui concerne les jeunes utilisateurs. Il s'agit, par exemple, de l'école qu'ils fréquentent, de leur sexe, etc. L'entreprise avait une très longue liste d'intérêts, et un grand nombre de ces intérêts concernaient les sorties, les fêtes, les soirées arrosées ou des choses que les jeunes ne veulent peut-être pas partager avec leurs parents ou d'autres adultes.

**L'hon. Lawrence MacAulay:** Mais ils l'écrivent quand même.

**M. John Lawford:** C'est un choix, et cette personne a accepté de le faire. Il y a aussi un grand nombre de forums gratuits; ils peuvent donc écrire à leurs amis, tout comme ils le font sur Facebook ou sur un autre site. À mon avis, une grande partie des renseignements sont seulement sensibles dans leur contexte.

**L'hon. Lawrence MacAulay:** Il y a aussi une grande différence entre avoir 14 ans et en avoir 24, et vous ne voulez pas que ces renseignements soient divulgués.

● (1600)

**M. John Lawford:** Ce que nous disions, en grande partie, c'est qu'il pourrait être raisonnable qu'un adulte de 24 ans fasse le choix conscient de divulguer ce type de renseignements sensibles dans un espace public, mais souvent, les adolescents n'ont pas la maturité nécessaire pour comprendre que ces renseignements seront aussi disponibles soit à l'extérieur du site Web, dans le cas de Nexopia, soit sur le site de l'entreprise.

**L'hon. Lawrence MacAulay:** Je présume donc qu'à votre avis, la commissaire à la protection de la vie privée devrait avoir le pouvoir de faire appliquer la loi.

**M. John Lawford:** Je l'ai dit et je le répète: oui.

**L'hon. Lawrence MacAulay:** Quelles sont les responsabilités des sites Web commerciaux et des sites comme Facebook, Twitter et Myspace lorsqu'il s'agit d'informer les gens de façon complète et transparente sur la façon dont leurs renseignements seront utilisés? Ou est-ce seulement un mythe? Est-ce que cela arrive parfois? Ou est-ce comme dans le cas du journaliste, c'est-à-dire que les renseignements sont là et on ne le dit pas aux gens?

**M. John Lawford:** Je pense que les sites Web de quelques entreprises réussissent mieux que d'autres à cet égard. Par exemple, Google essaie de son mieux. Cette entreprise est tellement grande et complexe qu'à mon avis, elle ne peut tout simplement pas exprimer clairement cette information. Mais nous constatons que lorsque les sites Web essaient de l'écrire en tenant compte du point de vue de l'utilisateur plutôt que de leur propre point de vue d'entreprise, les choses deviennent beaucoup plus claires. Lorsque les entreprises considèrent les fonctions que les gens utiliseront sur leur site Web, ces gens comprennent mieux que lorsqu'on leur dit que les entreprises pourraient utiliser les renseignements dans leur ensemble en vue de certaines utilisations commerciales et les communiquer à leurs sociétés affiliées. Et personne ne sait ce qu'est une société affiliée, n'est-ce pas? C'est possible d'y arriver. Il est très difficile d'élaborer une politique appropriée en matière de vie privée, mais je pense que cette responsabilité incombe aux entreprises, car elles obtiennent des renseignements personnels, c'est ce qui leur donne leur valeur, et elles ont donc la responsabilité de communiquer clairement leur politique.

**L'hon. Lawrence MacAulay:** Quelle relation les sites de réseautage social entretiennent-ils avec les responsables de la collecte des données?

**M. John Lawford:** Il y a plusieurs liens entre les sites de réseautage social et les responsables de la collecte des données. Nexopia, dans la partie commerciale de son site Web, informait les annonceurs que grâce à sa base de données, elle savait comment les adolescents réfléchissaient et dépensaient leur argent. Je suis certain que Facebook se sert de cette technique. C'est comme cela qu'elle fait la promotion de son PAPE, c'est-à-dire qu'elle affirme savoir ce que les gens veulent. C'est acceptable si tout le monde sait que les entreprises possèdent ces renseignements et qu'elles les utilisent conformément à ce qu'elles avaient dit.

**L'hon. Lawrence MacAulay:** Vers où se dirige-t-on? Le phénomène prend-il de l'ampleur? Le gouvernement devrait-il prendre plus de règlements?

**M. John Lawford:** Je pense qu'il y a beaucoup de bonnes choses dans notre loi. Toutefois, il faut lui apporter quelques rajustements. Il s'agit vraiment de veiller à ce que la commissaire à la protection de la vie privée examine ces problèmes, car elle est entourée des spécialistes nécessaires. Elle peut même prendre une longueur d'avance et collaborer avec d'autres commissaires à la protection de la vie privée dans le monde pour s'attaquer aux problèmes les plus urgents.

Nous n'avons pas vraiment besoin de modifier la loi; toutefois, une loi sur l'obligation de signaler les atteintes à la protection des données pourrait être utile. Mais il ne faut pas se contenter de prendre toujours plus de règlements.

**L'hon. Lawrence MacAulay:** Merci.

[*Français*]

**Le président:** Monsieur Calkins, vous disposez de sept minutes.

[*Traduction*]

**M. Blaine Calkins (Wetaskiwin, PCC):** Merci, monsieur le président, et merci, monsieur Lawford, d'être ici et du rôle que vous jouez dans la protection de l'intérêt public et des consommateurs. Votre rôle est essentiel.

Je vais vous poser des questions pour tenter de mieux comprendre certaines choses, car c'est très compliqué.

J'ai le privilège de connaître vos antécédents d'avocat et de conseiller juridique. Mes propres antécédents d'administrateur de bases de données et de programmeur m'ont permis d'acquérir une certaine expérience du sujet. Je n'ai jamais créé de système d'information lié aux médias sociaux, mais je m'occupais de grandes quantités de données d'entreprise.

Je pense que je vous ai interrompu lorsque vous avez parlé des quatre choses accomplies par la commissaire à la protection de la vie privée, et je m'en excuse. Vous avez précisé que les données représentaient l'actif le plus important d'un site de réseautage social. Je peux vous garantir que la valeur nette d'une organisation comme Facebook n'est pas dans les câbles et les ordinateurs, qui valent seulement quelques millions de dollars; elle se trouve plutôt dans les données qui, elles, valent des milliards de dollars. C'est donc l'avantage stratégique le plus important de n'importe quel site de réseautage social. Il s'agit probablement aussi de l'avantage stratégique le plus important de la plupart des entreprises — c'est-à-dire leurs consommateurs et les données qu'ils fournissent — et il est bien sûr visé par un grand nombre de lois et de règlements; cela ne devrait pas donc pas nous étonner.

Dans les premières recommandations, vous avez aussi mentionné que la commissaire à la protection de la vie privée n'avait pas le pouvoir de rendre des ordonnances et qu'elle devait faire appel aux tribunaux. Étant donné que vous êtes avocat, j'aimerais que vous m'expliquiez comment vous pouvez comparaître devant le comité en disant que vous souhaitez que la commissaire à la protection de la vie privée soit l'enquêteuse, le jury, et le juge et lui donner le contrôle de tout le processus, sans qu'un tribunal puisse exercer une certaine supervision pour équilibrer les choses.

J'ai déjà été un agent d'exécution de la loi. Je peux avouer que parfois, j'aurais aimé être le juge et le jury et administrer la peine, mais tout ce que je pouvais faire, c'était remplir mon rôle et porter des accusations contre les individus concernés en laissant le contrôle judiciaire suivre son cours; elle a une très bonne raison d'être.

Pourriez-vous donc m'expliquer pourquoi, selon vous, certains de ces cas les plus importants ne devraient pas faire l'objet de ce type de contrôle?

● (1605)

**M. John Lawford:** Je pense que oui. La structure actuelle de la loi permet à la personne qui a porté plainte ou à la commissaire à la protection de la vie privée de se rendre devant la Cour fédérale pour faire respecter le paiement d'une amende. L'entreprise ne peut pas se plaindre si elle perd. Cela fonctionne bien si la première résolution est du même type que celle prise par l'ombudsman lorsqu'il recommande un changement.

Si la commissaire devait devenir le juge, le jury et la personne qui applique la loi, et qu'elle pouvait infliger des amendes ou rendre une ordonnance, il faudrait, à mon avis, donner le droit à l'entreprise — si la décision est rendue par un tribunal — de se rendre devant la Cour fédérale pour soutenir qu'il s'agit d'une mauvaise décision. Je pense qu'il faudrait apporter ces modifications à la loi, car c'est injuste de ne pas avoir le droit de porter l'affaire en appel lorsqu'on vous accuse de ne pas respecter les règlements.

**M. Blaine Calkins:** Il s'agit absolument d'une question d'application régulière de la loi.

**M. John Lawford:** Je suis certainement de l'avis, moi aussi, qu'il faudrait apporter ce changement si l'on donnait le pouvoir de rendre des ordonnances. Par exemple, en Alberta, on peut s'adresser au Banc de la Reine pour dire que la décision rendue par le Commissariat à la protection de la vie privée est insensée et la faire annuler.

Si l'on veut séparer les deux fonctions — comme on le fait au Bureau de la concurrence, où le commissaire déclare: « C'est une mauvaise pratique », puis le Tribunal de la concurrence décide s'il a raison ou non —, il va falloir ajouter beaucoup de superstructure pour la protection de la vie privée. Il se peut qu'il soit nécessaire de le faire pour les grands dossiers. Peut-être que nous nous en allons dans cette direction, mais je n'en suis pas encore certain.

**M. Blaine Calkins:** Merci, ces renseignements sont utiles.

Je vais passer à un deuxième point, qui n'est pas très clair, je crois. La notion de « suppression », de « désactivation », a été abordée aujourd'hui. Ces deux termes ne sont pas synonymes. Par exemple, des sites Web vous demanderont si vous voulez désactiver votre compte. L'utilisateur pense peut-être qu'il supprime son compte, mais c'est faux. Les données contenues dans le compte existent encore; le compte a simplement été désactivé. Certains vous diront qu'il y a de bonnes raisons de conserver les données: personne ne peut créer un compte identique ou semblable à celui que vous venez de désactiver — il y aurait deux comptes pareils. Dans certains cas, cela pourrait être dans l'intérêt d'un consommateur: il devient impossible de faire du cybersquattage. Si le compte était supprimé, il serait facile de le faire.

De façon générale, je comprends pourquoi quelqu'un pourrait vouloir que des données soient supprimées d'une base de données. Si je ne voulais pas qu'une organisation possède certaines données à un certain moment, je pense que je lui ordonnerais ou je lui demanderais de les supprimer. Je comprends aussi la complexité d'avoir plusieurs copies de secours, que ces copies soient faites par sauvegarde statique ou dynamique. Comment peut-on modifier la copie obtenue par sauvegarde statique s'il faut procéder à une restauration en raison d'une défaillance du système? On ramènera des données qu'on ne pourra peut-être pas référencer à certaines étapes de la procédure de récupération.

C'est très difficile à faire, non seulement sur le plan législatif, mais aussi sur le plan technique. Pouvez-vous nous en dire plus sur des mesures que votre organisme a prises, nous conseiller sur ce qui a été fait ailleurs avec succès pour régler certaines affaires de ce genre?

**M. John Lawford:** J'aimerais pouvoir tout simplement vous mettre au courant, mais je sais qu'avec tout ce qui se passe en Europe sur la question du « droit à l'oubli », le groupe de travail « article 29 » étudie le dossier. J'ignore ce que leurs comités techniques font. Ce serait une très bonne idée de créer un comité, dirigé par la Commissaire à la protection de la vie privée et formé de représentants de l'industrie et d'autres intervenants, comme les groupes de défense des consommateurs, pour commencer à faire la même chose ici.

Vous avez raison: c'est très difficile. La question comprend de nombreux volets qui seront tous touchés, et pourtant, les consommateurs semblent ressentir le désir et le besoin de pouvoir supprimer certaines données.

Je crois que c'est faisable, mais il ne suffira pas d'adopter une loi qui dit qu'il doit y avoir une touche de suppression. Je pense que cela doit être fait avec la collaboration de tous, sinon, cela ne fonctionnera pas. Ce sera intéressant de voir ce qui va se passer en Europe; les Européens encouragent la discussion, mais au bout du compte, ils ont tendance à passer des lois. Nous verrons.

● (1610)

**M. Blaine Calkins:** Je ne sais pas si vous avez pu suivre les discussions que le comité a déjà tenues avec d'autres témoins. Lors de notre dernière séance, quelqu'un — je pense que c'était M. Zushman — a dit qu'avec ce que nous ne savions pas... J'ignore ce que je ne sais pas, et j'ignore ce que seront les technologies de l'avenir, même si je travaille dans le secteur de la technologie de l'information depuis nombre d'années.

Nous savons tous que les médias sociaux sont très bons pour afficher des photographies et pour d'autres types de logiciels. Avec les progrès de la technologie biométrique... Nous ne savons même pas ce que les futures technologies pourront faire des données affichées aujourd'hui. Certains consommateurs ne s'inquiètent peut-être pas de publier des données aujourd'hui, compte tenu de la technologie actuelle. S'ils savaient ce que l'avenir nous réserve, ils hésiteraient peut-être à afficher une photographie d'eux-mêmes aujourd'hui.

À cet égard, votre organisme s'est-il penché sur les répercussions des technologies futures sur la protection des consommateurs ou la sécurité publique?

**M. John Lawford:** Nous avons un peu abordé la question avec la plainte contre Nexopia, parce que si quelqu'un veut se créer un profil et afficher une photographie, Nexopia exige ou exigeait — je pense que c'est encore le cas — que la photo montre le visage ou le torse. Je ne sais pas exactement pourquoi le torse est inclus, mais le visage l'est certainement. L'obligation que les gens mettent une photo de leur visage pose évidemment un problème par rapport à la reconnaissance faciale, qui peut être exécutée sur un réseau. Pour nous, c'est une préoccupation.

Nous pourrions proposer au comité de recommander au Parlement qu'on ne devrait, dans aucun cas, être obligé d'afficher une photo de soi-même, de son visage, grâce à laquelle nous pourrions être identifiés par un logiciel de reconnaissance faciale — à moins que ce soit pour un passeport ou quelque chose du genre.

La question est intéressante. J'aimerais l'explorer plus à fond, mais je regrette, c'est tout ce que nous avons fait dans ce domaine.

[*Français*]

**Le président:** Merci.

Je vais maintenant céder la parole à Mme Borg pour cinq minutes.

**Mme Charmaine Borg (Terrebonne—Blainville, NPD):** Merci, monsieur le président.

Monsieur Lawford, je vous remercie d'être parmi nous aujourd'hui.

Vous avez très bien fait valoir qu'il y avait un manque concernant les pouvoirs de la commissaire. Comme l'a mentionné mon collègue M. Calkins, quand M. Zushman a fait un recours collectif pour déposer des plaintes contre Facebook, la commissaire a dû se tourner vers le tribunal pour régler le problème. Si elle doit avoir recours au tribunal, c'est peut-être qu'il lui manque des pouvoirs.

Certaines provinces permettent à leur commissaire d'imposer des amendes, notamment. Savez-vous comment ce modèle fonctionne, dans ces provinces? Pourrait-il être appliqué ici, au palier fédéral?

**M. John Lawford:** En Alberta, le commissaire peut recommander d'imposer une amende dans les cas d'atteinte à la protection des données. J'ai étudié une trentaine de ces décisions, et elles sont suffisamment efficaces pour modifier les pratiques des compagnies où il y a des problèmes, même lorsque l'amende est de 5 000 $ ou de 10 000 $.

Si on a le pouvoir et la responsabilité d'imposer des amendes, on prend des décisions suffisamment costaudes pour que les autres compagnies les étudient. Les décisions de ce commissaire sont en quelque sorte de petits essais sur l'atteinte à la protection des données qui bénéficient vraiment aux autres compagnies, en ce sens que ça leur évite de faire la même chose. Ce n'est qu'un exemple parmi d'autres.

**Mme Charmaine Borg:** Merci.

Vous avez parlé de l'enquête de la commissaire et des 24 recommandations qu'elles a faites au sujet de Nexopia. Corrigez-moi si je fais erreur, mais je crois que seulement quatre d'entres elles sont présentement considérées par la cour.

Qu'en est-il des vingt autres? Nexopia a-t-elle respecté les recommandations et les échéances?

● (1615)

**M. John Lawford:** À ce jour, Nexopia n'a rien fait, et la commissaire à la protection de la vie privée du Canada n'a rien dit. Je ne sais pas exactement pourquoi les deux échéances, soit le 30 juin et le 30 septembre, sont passées sans que rien ait été dit. J'imagine que quelque chose se passe à Nexopia ou que l'entreprise se penche là-dessus, mais on ne sait pas pourquoi ces gens continuent de ne pas respecter la conclusion de la commissaire.

**Mme Charmaine Borg:** Merci.

Pour certaines entreprises, il s'agit d'un modèle d'affaires. À votre avis, les entreprises qui font des affaires dans le domaine des données veulent-elles vraiment mettre en pratique ce qui se fait présentement pour protéger les renseignements personnels?

**M. John Lawford:** C'est difficile de répondre à cette question. Il ne s'agit pas de la volonté ou du désir des compagnies de respecter la loi; c'est plutôt que là où la loi est molle, on va jusqu'au bout. C'est normal. On le fait pour faire des affaires de façon efficace.

Par contre, dans le cas de Nexopia, Facebook ou la CIPPIC, certaines personnes ont encore des problèmes. Pour ce qui est de Facebook, on a constaté que des fuites de données étaient liées à certaines applications. Or la position de cette compagnie consiste à dire que comme c'est fait par des tierces parties, elle n'est pas responsable. Ce problème n'est toujours pas résolu, je crois.

Pour régler les problèmes, il s'agit essentiellement de clarifier les lois et de les faire appliquer.

**Mme Charmaine Borg:** Je vais changer de sujet.

Vous avez indiqué que les données pouvaient être « désidentifiées » et « réidentifiées » par la suite. Peut-on se pencher sur une solution potentielle pour s'assurer que les données restent anonymes ou, du moins, que les consommateurs puissent comprendre le processus de « désidentification » et de « réidentification »?

**M. John Lawford:** Le comité a fait témoigner des experts dans le domaine de la santé, et ces questions ont été abordées très minutieusement, si je puis dire.

De plus, si la commissaire à la protection de la vie privée du Canada était convoquée de nouveau par le comité, on pourrait lui demander si des lignes directrices seront établies.

**Mme Charmaine Borg:** Merci.

**Le président:** Je vais donner la parole à M. Mayes.

Vous disposez d'un peu plus de cinq minutes puisque vous êtes la dernière personne à poser des questions.

[*Traduction*]

**M. Colin Mayes (Okanagan—Shuswap, PCC):** Merci, monsieur le président.

Merci, monsieur Lawford, d'être ici aujourd'hui et de nous faire part de vos connaissances dans le domaine. Vous trouverez peut-être mes questions un peu simplistes, comparativement à celles de mon collègue, M. Calkins, qui s'y connaît bien dans le domaine.

Pendant votre déclaration préliminaire, vous avez parlé de « renseignements personnels » et de « renseignements généraux ». Ces termes sont-ils bien définis? Les lignes directrices qui expliquent la différence entre les deux sont-elles assez claires?

● (1620)

**M. John Lawford:** Je pense que oui. C'est intéressant, parce qu'au Canada, la LPRPDE contient une définition du terme « renseignement personnel », et tout le monde veut l'éviter parce qu'elle est tellement claire. Selon cette définition, tout renseignement concernant un individu identifiable est un renseignement personnel. C'est très vaste. Dans beaucoup de ses décisions, la commissaire à la protection de la vie privée a dit que cela incluait presque tout. Cela inclut les paiements nets faits sur votre ordinateur. Dans certains cas, cela inclut votre adresse IP. Cela inclut la couleur de vos cheveux, de vos yeux, votre poids, tout.

Malheureusement, un grand nombre de politiques de confidentialité sont conçues par des avocats américains pour des entreprises américaines qui font des affaires au Canada. La règle n'est pas la même là-bas — on parle de renseignement d'identification d'une personne —; ils ont donc tendance à ne pas adapter suffisamment les politiques pour le Canada.

**M. Colin Mayes:** Certaines de nos discussions ont porté sur les avertissements au sujet des conditions d'utilisation de sites Web. J'ai trouvé intéressant que vous parliez d'une liste d'interdiction de suivi. Je me demande s'il serait possible d'obliger les sites à avoir une période de rétention des données; il faudrait que l'utilisateur accepte cette période de rétention des données, et ce serait écrit noir sur blanc à l'écran, premièrement. Ou cela pourrait être un peu plus simple: l'utilisateur autorise-t-il, oui ou non, la communication ou la vente de ses renseignements personnels? Les choses de ce genre sont très simples et les gens peuvent les comprendre, les gens comme moi qui ont une compréhension limitée de ce type d'utilisations. Je suis certain qu'il est possible d'apporter des améliorations sur ce plan.

Vous avez parlé de renforcer l'application. Or, l'application est coûteuse. Pour qu'elle soit bien faite, il faut des ressources humaines et financières. Avez-vous songé à qui devrait assumer les frais? Devrait est-ce le serveur, le contribuable ou un organisme de réglementation quelconque?

**M. John Lawford:** Nous y avons songé un peu. C'est pour cette raison que j'ai mentionné, à la fin, que le comité pourrait se pencher sur la liste de numéros de télécommunication exclus ou le modèle anti-pourriel. Il y a des coûts rattachés aux numéros exclus, pour acheter les listes. Pour la Loi anti-pourriel, les amendes vont au CRTC, pour qu'il continue à la faire respecter. Un de ces deux modèles pourrait aider.

J'aimerais revenir en arrière, parce que pour moi, l'application — et je pense que c'est de cette façon que le CRTC procède pour la liste de numéros exclus — peut être beaucoup de choses. On peut commencer par des avis et de petites amendes; on peut s'adresser à des associations commerciales. Il y a beaucoup de choses qu'on peut faire avant de sortir les gros canons et de passer aux mesures coûteuses. Même si le problème n'est pas facile à régler, j'espère que ce ne serait pas aussi coûteux que la liste d'interdiction de suivi ou de numéros exclus.

**M. Colin Mayes:** Est-ce que les gens déposeraient des plaintes ou est-ce qu'il y aurait des enquêtes et de la surveillance?

**M. John Lawford:** Ce serait la même chose que pour tout domaine d'application, comme la sécurité. On recevrait des plaintes et des informations, mais il faudrait qu'un organe d'application travaille à ses propres enquêtes.

Je pense que la commissaire à la protection de la vie privée a fait tout ce que son budget lui permet de faire. Le commissariat n'a pas été très agressif dans ses vérifications d'entreprises, qui est un de ses pouvoirs. Il n'a pas vraiment pris l'initiative de lui-même. On pourrait l'encourager à le faire.

**M. Colin Mayes:** Comment conciliez-vous le traitement des renseignements personnels par les médias sociaux avec des choses comme les vérifications de la solvabilité et la collecte de données personnelles par les compagnies d'assurances?

Si, pour une raison quelconque, je ne paie pas une facture à un moment donné, et l'entreprise a une politique de recouvrement agressive et ajoute cela à ma cote de solvabilité, qui est peut-être une cote AAA, et je n'en sais rien, c'est peut-être là des données non fondées dont je ne suis pas au courant. Comment conciliez-vous cela avec ce genre d'utilisations?

**M. John Lawford:** C'est intéressant, parce que les rapports sur les consommateurs ou les rapports de solvabilité, dont vous parlez, ont précédé les lois sur la protection de la vie privée. Comme vous le savez, les lois provinciales contiennent quelques mesures de protection. Par exemple, la personne peut corriger les renseignements ou elle peut au moins insérer une note dans son dossier pour indiquer qu'il y a une erreur.

Quand les lois sur la protection de la vie privée ont été révisées ici à la fin des années 1990, nous avons dit que le modèle n'était pas assez bon. Le comité qui travaillait à la LPRPDE en a beaucoup parlé. Ces mesures ne suffisaient pas. Il faut donner à la personne le droit d'exiger que les renseignements soient changés, et c'est maintenant compris dans la loi.

Vous avez raison. Le truc, c'est d'informer les gens de leur droit. Puis, comment procède-t-on pour que ce soit facile à faire et à corriger au sein d'une grande entreprise complexe?

Je ne crois pas que les réseaux sociaux le feront. Ce n'est pas facile d'enlever un élément de donnée ou de corriger une seule chose.

● (1625)

**M. Colin Mayes:** Personnellement, je pense que si une entreprise a l'intention de signaler quelque chose qui nuira à ma cote de solvabilité, je devrais en être informé. Non seulement le renseignement est envoyé, mais j'en suis avisé. N'est-ce pas raisonnable?

**M. John Lawford:** Oui, et cela me fait penser à ce qu'on essaie de faire en Europe en donnant aux utilisateurs un peu plus de contrôle des renseignements qui leur sont nuisibles, en leur permettant de les supprimer ou de les vérifier. Le simple fait de dire qu'on a le droit d'avoir des données exactes... Eh bien, qui prend le temps de vérifier ses données, comme vous l'avez dit? Aussi, certaines données sont si délicates qu'il y a des répercussions si elles sont fausses. Je ne sais pas vraiment comment corriger cela.

**M. Colin Mayes:** Vous n'êtes peut-être pas au courant des données qu'un créancier transmet à une agence d'évaluation du crédit.

**M. John Lawford:** Non, et encore une fois, en ce qui touche les réseaux sociaux, le seul parallèle, c'est lorsque vous identifiez vos données et qu'elles sont envoyées à un tiers, ou lorsque la politique de confidentialité donne la permission au site Web de communiquer vos renseignements à des tiers, mais que vous ne l'avez pas lue ou que vous ne l'avez pas comprise, et que vos données sont transmises. C'est à peu près la même chose.

Je pense qu'un site de réseautage social dirait que vous avez inclus vos données et que vous saviez qu'elles pourraient être transmises à d'autres. Avec les rapports de solvabilité, ce n'est pas la même chose parce que vous n'êtes pas averti. Or, si vous jetez un coup d'oeil à votre demande de crédit, vous verrez, bien sûr, que c'est écrit qu'on procéderait ainsi.

[*Français*]

**Le président:** Merci, monsieur Mayes. Votre temps de parole est écoulé.

J'apprends que M. Boulerice a une brève question à poser. Je vais donc lui donner deux minutes pour la poser.

**M. Alexandre Boulerice (Rosemont—La Petite-Patrie, NPD):** Monsieur le président, vous êtes d'une générosité exemplaire.

Merci beaucoup d'être parmi nous, monsieur Lawford. C'était fort intéressant et pertinent.

J'ai deux questions à vous poser. Je vous prierais de répondre à ma première question par oui ou non. S'il y a une atteinte aux données, c'est la compagnie même qui décide de rapporter les faits ou non à la commissaire à la protection de la vie privée du Canada. Ai-je bien compris?

**M. John Lawford:** Pour l'instant, la réponse est oui, conformément aux lignes directrices de la commissaire.

C'est aussi ce que prévoit le projet de loi C-12, mais cela n'a pas encore force de loi.

**M. Alexandre Boulerice:** Selon moi, cela n'a pas de sens. Je suis très réticent à avoir recours à l'autorégulation pour ce genre de choses. Je trouve cela un peu troublant.

Je vais maintenant jouer un peu à l'avocat du diable. Ma deuxième question exclut les enfants et les adolescents. La plupart des médias sociaux sont essentiellement basés sur le fait de mettre des éléments de sa vie privée sur la place publique. En tant que législateur, comment fait-on pour protéger les renseignements personnels des gens quand le modèle d'affaires est basé sur le partage de renseignements personnels?

**M. John Lawford:** En effet, l'intention est bien celle-là. Vous voyez, dans ces séances, le jeu qui se joue entre les deux parties, entre le but de ces sites et le but de cette loi. Pour l'instant, on dit que le consentement nous permet de décider où se trouve la limite. Le problème est que les conditions pour donner son consentement ne sont pas assez claires.

**Le président:** C'est ce qui conclut la période de témoignage.

Merci beaucoup de votre présence, monsieur Lawford.

On va suspendre la séance pour quelques minutes, puisque la prochaine partie de la réunion est à huis clos.

Encore une fois, merci.

Aux membres du comité, je dis à tout à l'heure.

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