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 052 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mardi 21 mars 2017

Président

M. Blaine Calkins

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

Le mardi 21 mars 2017

● (1605)

[*Traduction*]

Le président (M. Blaine Calkins (Red Deer—Lacombe, PCC)): Bienvenue, chers collègues. Merci d'être de bonne humeur malgré les manigances qui ont lieu à la Chambre actuellement.

Je remercie les témoins de leur patience. Le processus démocratique n'est pas toujours net et ordonné. C'est parfois difficile, mais il n'en demeure pas moins que c'est le meilleur système que nous puissions avoir.

Nous avons un peu plus d'une heure. Nous devrons probablement terminer la séance vers 17 h 15, à moins qu'il y ait consentement unanime pour que nous poursuivions nos travaux après que la sonnerie se soit fait entendre, à peu près à cette heure-là. Il nous faudra environ 40 minutes pour entendre tous les témoins, puis 30 minutes supplémentaires pour la première série de questions. C'est probablement tout ce que nous aurons le temps de faire, à moins que nous en décidions autrement à ce moment-là.

Nous allons entreprendre notre 52e réunion sans plus tarder. Nous poursuivons notre étude de la Loi sur la protection des renseignements personnels et les documents électroniques, la LPRPDE.

Aujourd'hui, nous accueillons Mme Micheal Vonn, qui est directrice de la politique. Bienvenue au comité encore une fois, Micheal. Nous sommes heureux de vous revoir.

Nous avons M. Michael Geist, qui témoigne à titre personnel et qui est un habitué. Bon retour parmi nous, Michael.

Témoignant à titre personnel, nous avons M. David Fraser — un autre habitué — et M. Colin Bennett. Merci beaucoup de vous joindre à nous.

Si cela vous convient, vous témoignerez dans l'ordre auquel je vous ai présentés.

Oui, monsieur Kelly.

M. Pat Kelly (Calgary Rocky Ridge, PCC): Monsieur le président, je sais que la réunion d'aujourd'hui est considérablement écourtée, mais j'aimerais proposer que le comité invite le président du Conseil du Trésor, l'honorable Scott Brison, à comparaître au comité le plus tôt possible pour discuter de sa décision récente de reporter la réforme de la Loi sur l'accès à l'information.

J'aimerais en faire la proposition maintenant.

Le président: Présentez-vous la motion, ou s'agit-il d'un avis de motion de 48 heures?

M. Pat Kelly: C'est un avis de motion.

Le président: C'est bien, monsieur Kelly, car un avis de 48 heures est requis pour toute motion de fond.

M. Pat Kelly: En effet. Je présente un avis maintenant.

Le président: Un avis de motion a été donné. Merci beaucoup.

Nous passons maintenant à...

M. Matt Jeneroux (Edmonton Riverbend, PCC): Cela peut-il faire l'objet d'un débat?

Le président: Non; la motion sera présentée dans 48 heures.

Revenons à l'ordre du jour. Nous passons à Mme Micheal Vonn, pour 10 minutes tout au plus.

Mme Micheal Vonn (directrice de la politique, Association des libertés civiles de la Colombie-Britannique): L'Association des libertés civiles de la Colombie-Britannique est un organisme non partisan dont le mandat est de défendre les libertés civiles et les droits de la personne au Canada. La protection des renseignements personnels est l'un de nos plus importants dossiers. Nous vous remercions de nous donner l'occasion de comparaître dans le cadre de l'examen de la LPRPDE.

Je tiens d'abord à souligner que nous n'avons pas eu l'occasion d'étudier assez attentivement le RGPD pour présenter des observations sur l'examen prochain concernant sa pertinence. C'est donc de bonne grâce que nous laissons aux autres témoins le soin de présenter des observations à cet égard.

Notre association appuie et réitère les recommandations et les préoccupations déjà exprimées par les universitaires, les organismes de réglementation et les témoins de la société civile. À titre d'exemple, nous appuyons fermement la mise en place de pouvoirs d'application considérables dans la LPRPDE, en particulier le pouvoir de rendre des ordonnances, la capacité d'imposer des amendes et d'accorder une indemnité aux plaignants lorsque les circonstances le justifient.

Nous réclamons de tels pouvoirs depuis plus d'une décennie. Nous sommes d'avis qu'il n'y a plus d'argument crédible justifiant le maintien du modèle de l'ombudsman, étant donné que les entités provinciales ont, depuis longtemps, démontré que les pouvoirs d'ordonnance peuvent être efficaces lorsque combinés à des enquêtes coopératives, la médiation et la sensibilisation.

De même, nous joignons notre voix à d'autres organismes, dont la BC Freedom of Information and Privacy Association, pour demander que les partis politiques fédéraux soient assujettis à la LPRPDE, comme cela se fait en Colombie-Britannique, où les partis politiques provinciaux sont visés par la loi provinciale correspondante.

De nombreux Canadiens — en particulier ceux des régions au centre des divers scandales liés aux appels automatisés — nous ont indiqué que l'absence de mesures visant à réglementer la collecte, l'utilisation et la divulgation des renseignements personnels détenus par les partis politiques fédéraux est totalement inacceptable. Il s'agit d'un enjeu d'une importance et d'une urgence capitales, pour des raisons évidentes, notamment les abus survenus dans le passé qui ont facilité la fraude électorale.

J'aimerais parler brièvement d'un enjeu qu'on appelle le « droit à l'oubli » ou, de façon plus générale, de la question de la réputation en ligne. Cet enjeu touche des droits contradictoires. Notre association n'a pas encore de position officielle à cet égard, mais elle demeure au fait des demandes et des intérêts contradictoires. Nous aimerions donc apporter quelques précisions à ce sujet.

Premièrement, il convient de comprendre le contexte dans lequel s'inscrit cette discussion. Nous sommes d'avis qu'il faut rejeter la notion selon laquelle nous avons affaire à une situation comparable au fait de détruire une fiche du catalogue sur fiches d'une bibliothèque, la comparaison habituelle pour le déréférencement.

En tout lieu et en tout temps, il n'a jamais été possible de demander qu'une bibliothèque collecte les renseignements sur un voisin qui n'était pas une personnalité publique et dont les activités n'étaient pas d'intérêt public ou dignes d'un intérêt quelconque. Jusqu'à tout récemment, la vie privée de la grande majorité des membres du public ou des gens ordinaires — locataires, collègues de travail, anciens partenaires d'un partenaire actuel, camarades de classe, connaissances — était protégée par l'obscurité pratique. L'avènement d'Internet et de puissants moteurs de recherche a entraîné une érosion considérable de cette protection, et il va sans dire que des gens ont subi des préjudices.

Permettez-moi de vous donner un exemple d'un cas lié à la réputation en ligne survenu en Colombie-Britannique. Une petite entreprise de Nanaimo a eu un long conflit avec Google concernant les obligations de la société, en vertu de ses propres politiques, quant au retrait des critiques anonymes en ligne. Cela englobe les attaques personnelles diffamatoires à l'égard des employés d'une entreprise. Une employée, que j'appellerai Mme Jones, a fait l'objet de commentaires selon lesquels elle est une personne raciste qui a une durée d'attention comparable à celle d'un insecte xylophage. L'incapacité de l'entreprise à obtenir le retrait des attaques personnelles anonymes à l'égard des employés a fait l'objet d'un reportage de la CBC. En fait, il semble que seules la publicité négative et la médiatisation de l'affaire aient incité Google à retirer ces critiques.

Dans ma préparation en vue de ma comparution au comité, j'ai dû revoir les faits entourant cette affaire, qui a fait l'objet d'un reportage dans les médias. J'ai trouvé l'article en question en faisant une recherche dans Internet à l'aide des termes de recherche suivants: « Google, B.C., online review, personal attack ». J'ai trouvé l'article, comme il se doit. On y trouvait les renseignements sur Mme Jones, comme il se doit, encore une fois.

● (1610)

Ensuite, j'ai fait une expérience. J'ai fait une recherche en utilisant simplement « Ms. Jones » comme terme de recherche, comme pourrait le faire un voisin curieux, un employeur potentiel, un propriétaire ou un client. Le premier résultat de recherche était l'article à son sujet où elle était la cible d'une attaque personnelle, où elle était décrite comme une personne raciste atteinte de déficience cognitive.

Est-ce ainsi que cela devrait être?

Si cela pose problème — et nous savons que c'est le cas, car des gens communiquent avec nous pour trouver des solutions à ce problème précis —, comment peut-on le régler sans miner d'autres droits essentiels comme le droit à l'accès à l'information et le droit à la liberté d'expression? Selon nous, la tenue de discussions à ce sujet ne peut se faire sans définir clairement le problème. Le problème n'est pas que des recherches en ligne me mènent à des renseignements sur Mme Jones, mais plutôt que des recherches sur Mme Jones me mènent à des articles sur la réputation en ligne qui font état de commentaires diffamatoires à son égard.

Sans vouloir étudier les solutions possibles pour régler ce problème précis, il semble à tout le moins prématuré d'affirmer que toute solution serait nécessairement inconstitutionnelle. L'espoir est certainement de trouver une solution qui protège l'ensemble des droits qui sont en jeu.

En terminant, je tiens à traiter du recours à ce qu'on appelle les « évaluations éthiques » ou les « cadres éthiques » pour les mégadonnées et l'Internet des objets. Comme le CPVP l'a indiqué dans son aperçu des mémoires reçus dans le cadre de la consultation sur le consentement, les entreprises et l'industrie sont très favorables au recours à des cadres éthiques relatifs à l'utilisation des renseignements personnels, que ce soit à titre de niveau supplémentaire de responsabilité ou, ce qui est plus probable, comme mesure compensatoire pour un système caractérisé par l'érosion du consentement.

La question de savoir s'il est possible de donner une valeur significative au consentement — et la façon d'y arriver, le cas échéant — nécessite évidemment un vaste débat. Pour le moment, je me contenterai de dire que le modèle d'évaluation proposé n'est pas éthique. Lui donner le nom de « cadre éthique » pose un grave problème.

Dans ce cadre, il incombera à ceux qui veulent utiliser les données pour en tirer profit de déterminer s'il est justifié de le faire, en fonction des risques en matière de protection des renseignements personnels, des atteintes à la réputation, etc. Or, ces risques sont assumés par d'autres. Donc, ceux qui pourraient en tirer profit seront chargés d'établir le niveau de risque et de déterminer si leurs fins l'emportent sur les risques allégués. Les personnes qui sont exposées à ces risques n'ont pas voix au chapitre.

Il est tout simplement impossible d'affirmer qu'une telle répartition des avantages et des risques est éthique. De toute évidence, beaucoup de gens consciencieux s'acquitteront de cette tâche de façon éthique et équitable. Cela dit, abstraction faite des personnes en cause, le processus lui-même revient manifestement à demander au loup de protéger la bergerie, avec comme seule promesse d'agir de façon éthique. Comme vous le constaterez en examinant les notes du CPVP, leur sens éthique ne va pas jusqu'à souhaiter qu'un tiers désintéressé, un comité d'éthique indépendant, par exemple, joue un rôle quelconque dans cette protection.

En résumé, notre message pour le Comité est que nous considérons que la solution des cadres éthiques n'est aucunement éthique et n'est pas une solution.

Merci beaucoup.

● (1615)

Le président: Merci beaucoup.

Nous passons maintenant à M. Michael Geist.

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

Bonjour. Je m'appelle Michael Geist. Je suis professeur de droit à l'Université d'Ottawa et je suis titulaire de la chaire de recherche du Canada en droit d'Internet et du commerce électronique. Je comparais aujourd'hui devant votre comité à titre personnel et je ne représente que ma propre opinion.

Si j'avais plus de temps, je pourrais discuter de beaucoup d'autres enjeux, notamment l'application plus rigoureuse de la loi grâce au pouvoir d'ordonnance; la possibilité d'utiliser la Loi canadienne anti-pourriel comme modèle, à tout le moins pour les questions liées à l'application plus rigoureuse de la loi et aux normes de consentement; les préoccupations croissantes selon lesquelles les règles régissant le droit d'auteur pourraient miner la protection de la vie privée. Toutefois, étant donné le temps limité dont je dispose, je me concentrerai sur trois enjeux dans mon exposé d'aujourd'hui: les pressions pour une réforme de la Loi sur la protection des renseignements personnels, le consentement et la transparence.

Parlons d'abord de la réforme. J'ai eu l'honneur de comparaître devant des comités de la Chambre et du Sénat dans le cadre de l'étude du projet de loi S-4, qui était manifestement un effort visant à moderniser la LPRPDE grâce à la mise en oeuvre de recommandations remontant à 2006. Il était déjà évident, à l'époque, que d'autres modifications étaient nécessaires. En fait, le report continu de la mise en oeuvre de certaines dispositions de ce projet de loi, notamment celles sur le signalement des atteintes à la sécurité des données, témoigne de la lenteur accablante qui caractérise le processus de modernisation des lois canadiennes en matière de protection de la vie privée.

Je crois qu'il est plus urgent que jamais de régler le problème. Certains témoins vous ont déjà parlé — il pourrait y en avoir d'autres — des développements survenus en Europe concernant le RGPD, qui pourraient menacer le caractère adéquat attribué au Canada par les autorités européennes chargées de la protection de la vie privée.

Il convient toutefois d'attirer votre attention sur un autre développement à l'échelle internationale qui pourrait avoir, à mon avis, une incidence considérable sur les lois canadiennes en matière de protection de la vie privée: nos accords commerciaux et les négociations à cet égard. Il semble probable que la renégociation prochaine de l'ALENA puisse inclure une demande des États-Unis voulant que le Canada renonce à l'adoption de règles en matière de ce qu'on appelle la localisation des données, exigeant la conservation des renseignements personnels dans des serveurs informatiques situés au Canada. La localisation des données est une mesure stratégique de plus en plus utilisée par les pays en réaction aux préoccupations concernant la surveillance américaine et la subordination des mesures de protection de la vie privée pour les citoyens et les résidents non américains sous l'administration Trump.

En réponse à ces préoccupations croissantes, les grandes sociétés de technologie comme Microsoft, Amazon et Google ont établi en sol canadien des serveurs informatiques permettant la localisation des données, ou ont convenu de le faire. Ces mesures font suite à la stratégie sur l'infonuagique adoptée par le gouvernement fédéral en 2016, qui exigeait la conservation de certaines données au Canada.

Lorsqu'on étudie le Partenariat transpacifique, le PTP, on constate qu'il comportait des restrictions sur l'adoption d'exigences en matière de localisation des données, répondant ainsi aux pressions des négociateurs américains. Il semble que de telles dispositions seront réclamées lors des négociations entourant l'ALENA.

À mon avis, ce sera également le cas des restrictions sur le transfert de données, qui exigent la libre circulation de l'information sur les réseaux des deux côtés de la frontière. Ces règles sont évidemment d'une grande pertinence pour protéger les libertés en ligne dans des pays qui ont l'habitude de réprimer la liberté d'expression en ligne. Dans le contexte canadien, toutefois, de telles règles pourraient restreindre la capacité d'adopter des mesures de protection de la vie privée. En fait, si l'Union européenne exigeait la mise en place de restrictions sur les transferts de données, comme beaucoup d'experts s'y attendent, le Canada pourrait se retrouver dans une situation intenable à cet égard, soit une situation où l'Union européenne imposerait l'adoption de restrictions interdites par l'ALENA.

Le deuxième point est le consentement. Comme vous le savez, à l'échelle de la planète, les lois sur la protection de la vie privée sont différentes sur certaines questions, mais elles sont fondées sur un principe commun: la collecte, l'utilisation et la divulgation des renseignements personnels nécessitent le consentement de l'utilisateur. Ce principe est de plus en plus difficile à appliquer dans un monde numérique où les données sont recueillies de façon continue et peuvent être utilisées d'une myriade de façons inimaginables auparavant.

Au lieu d'affaiblir ou d'abandonner les modèles de consentement, je crois qu'il faut moderniser l'approche du droit canadien en rendant le consentement plus efficace dans l'environnement numérique. Il semble évident que le modèle actuel s'appuie encore trop sur des politiques de consentement présumé, en vertu desquelles les entreprises ont le droit de tenir pour acquis qu'elles peuvent utiliser les renseignements personnels de leurs clients à moins que ceux-ci ne les informent de leur refus. De plus, toute politique de protection des renseignements personnels qui entraîne de la confusion chez les membres du public quant à la façon dont leurs renseignements peuvent être recueillis ou divulgués crée une notion de consentement qui relève souvent de la fiction et non de la réalité.

Comment combler certaines lacunes du modèle actuel fondé sur le consentement? Premièrement, nous devrions mettre en oeuvre un système de consentement à adhésion facultative comme approche par défaut. À l'heure actuelle, l'adhésion facultative n'est utilisée que lorsqu'elle est strictement exigée par la loi ou que des renseignements de nature très délicate sont en cause, notamment pour les renseignements sur la santé ou les données financières. Cela signifie que la plupart des renseignements sont recueillis, utilisés et divulgués sans consentement éclairé.

Deuxièmement, comme le consentement éclairé dépend de la compréhension par les membres du public de la façon dont leurs renseignements seront recueillis, utilisés et divulgués, les règles associées à la transparence doivent être améliorées. Les cases à cocher comportant une possibilité de refus, qui entraînent de la confusion chez les membres du public en ce qui a trait à l'exercice du droit à la vie privée, devraient être rejetées comme forme appropriée de consentement. Les gens ne savent jamais s'ils doivent cocher ou décocher une case pour protéger leur vie privée.

● (1620)

De plus, étant donné l'incertitude associée aux mégadonnées et aux transferts transfrontaliers de données, il faut établir de nouvelles politiques en matière de transparence et de protection des renseignements personnels. Par exemple, la transparence algorithmique exigerait que les moteurs de recherche et les entreprises de médias sociaux divulguent la façon dont l'information est utilisée pour déterminer le contenu affiché à chaque utilisateur. En vertu de la transparence relative au transfert des données, les entreprises seraient tenues de communiquer le lieu de stockage des renseignements personnels et le transfert des données à l'extérieur du pays.

Troisièmement, le consentement effectif signifie de donner aux utilisateurs la capacité d'exercer leurs choix en matière de protection de la vie privée. La plupart des politiques sont offertes selon le modèle « à prendre ou à laisser », et on ne peut pas vraiment personnaliser la méthode de collecte, d'utilisation et de communication des renseignements. Le consentement réel devrait donner lieu à un choix réel.

Quatrièmement, il faut accroître les pouvoirs d'exécution pour lutter contre les atteintes à la vie privée. Les entreprises canadiennes se sont conformées rapidement aux lois antipourriel parce que ces lois étaient associées à d'importantes sanctions en cas de violation. La loi canadienne en matière de protection de la vie privée se fonde encore en grande partie sur la persuasion ou sur la peur de l'humiliation publique, et non sur l'exécution associée à des sanctions. Pour que les règles sur la protection de la vie privée soient prises au sérieux, il faut que les entreprises subissent de graves conséquences en cas de non-respect de la loi.

Enfin, j'aimerais aborder la question de la transparence et de l'établissement de rapports. Comme nombre d'entre vous le savent, au cours des dernières années, les révélations troublantes au sujet des demandes d'accès à l'information et de la communication des renseignements personnels des Canadiens — des millions de demandes, dont la majorité n'ont pas fait l'objet d'une intervention du tribunal et n'ont pas été associées à la délivrance d'un mandat — font état de la faiblesse très troublante des lois du Canada en matière de protection de la vie privée. En termes simples, la plupart des Canadiens ne savent pas que ces renseignements sont communiqués et sont surpris d'apprendre que cette pratique est courante.

Depuis peu, le secteur privé met l'accent sur l'établissement de rapports sur les mesures de transparence. De grandes entreprises Internet comme Google et Twitter ont présenté des rapports à cet égard. Twitter a lancé son 10e rapport annuel aujourd'hui, et d'autres grandes sociétés de communication du Canada comme Rogers et Telus ont emboîté le pas.

Malgré la présence d'une telle norme en matière de production de rapports sur les mesures de transparence, qui a été approuvée par le gouvernement et le commissaire à la protection de la vie privée, il y a encore des réfractaires. Le problème réside dans l'approche non contraignante en matière de transparence.

J'ai obtenu certains renseignements en vertu de la Loi sur l'accès à l'information, et j'ai appris qu'à la suite d'une réunion de tous les intervenants de l'industrie organisée par le commissaire à la protection de la vie privée en avril 2015, Rogers avait souligné ce qui suit:

> Lors de la réunion, on a fait valoir que les lignes directrices adoptées ne constitueraient pas un règlement, mais serait beaucoup plus imposantes que les lignes directrices volontaires.

Or, si l'approche non réglementaire ne fonctionne pas, il revient au commissaire fédéral à la protection de la vie privée ou au gouvernement d'agir.

Parmi les sociétés qui ne respectent pas ces normes en matière de transparence, la plus importante est Bell Canada, la plus grande entreprise de télécommunication du Canada. Au départ, Bell avait fait valoir qu'elle attendait que le commissaire à la protection de la vie privée établisse une norme à cet égard, mais aujourd'hui, près d'un an après l'établissement d'une telle norme, Bell n'a toujours pas publié son rapport sur les mesures de transparence. Des millions de Canadiens ne savent toujours pas quand, dans quelles circonstances et selon quelle fréquence Bell communique les renseignements personnels de ses clients. À mon avis, c'est tout simplement inacceptable.

Si la loi actuelle n'exige pas la communication de ces renseignements, alors la loi est problématique et il faudrait la réformer afin d'exiger la production de rapports sur les mesures de transparence et de prévoir des sanctions pour le non-respect de la loi. Vous savez comme moi qu'il ne se passe pas une journée sans qu'on entende parler d'un enjeu en matière de protection de la vie privée dans les médias. Je crois qu'il est évident que la population s'inquiète de la protection de la vie privée et que les entreprises commencent à reconnaître la valeur des renseignements personnels. Il est temps que la loi s'adapte à cette réalité.

Je serai heureux de répondre à vos questions.

● (1625)

Le président: Merci beaucoup.

La parole est maintenant à M. Fraser. Allez-y, monsieur.

M. David Fraser (associé, McInnes Cooper, à titre personnel): Bonjour. Je vous remercie, mesdames et messieurs les membres du Comité et monsieur le président, de me donner l'occasion de témoigner devant vous aujourd'hui sur ce sujet très important.

Je vais me présenter, rapidement. Je suis un avocat spécialiste de la protection de la vie privée et un associé chez McInnes Cooper, à Halifax. Je pratique le droit dans ce domaine depuis 15 ans, et je m'intéresse beaucoup à l'intersection ou à la collision entre les technologies et les droits civils depuis un bon moment. Je suis également membre à temps partiel de la faculté de droit de l'Université Dalhousie, où j'enseigne notamment le droit d'Internet et des médias, le droit et la technologie, et le droit relatif au respect de la vie privée. J'ai été président de l'Association canadienne du droit des technologies et de l'information et président de la Section nationale du droit de la vie privée et de l'accès à l'information de l'Association du Barreau canadien.

Mon point de vue est celui d'une personne qui conseille régulièrement les entreprises sur le respect des lois canadiennes en matière de protection de la vie privée. J'ai aussi représenté plusieurs sociétés et clients dans les cas d'enquêtes du Commissariat à la protection de la vie privée du Canada.

Au cours de cette période, j'ai eu l'occasion de conseiller mes clients au sujet d'un large éventail de questions en matière de protection de la vie privée, d'accès à l'information et de technologies. J'ai aussi souvent été exposé aux lois sur la protection de la vie privée des autres administrations. Au cours de ces 15 années de travail, j'ai constaté une chose: plus j'en apprends au sujet des lois sur la protection de la vie privée des autres pays, plus j'aime la loi canadienne. Elle est un exemple de neutralité technologique et de résilience. Elle a été rédigée dans les années 1990, mais est toujours très pertinente, surtout depuis qu'on a apporté des modifications par l'entremise de la Loi sur la protection des renseignements personnels numériques.

Je souligne que mes commentaires ne reflètent pas l'opinion de mon cabinet, de mes clients ou des organisations pour lesquelles je travaille. Il s'agit de mon point de vue et de mon opinion personnels.

Pour ce qui est des détails, j'aimerais aborder trois questions, mais je serai heureux de discuter de tous les sujets que vous aborderez au cours de la période de questions.

Tout d'abord, j'aimerais parler du droit à l'oubli. J'aimerais ensuite parler des pouvoirs du commissaire à la protection de la vie privée. Enfin, j'aimerais aborder la question du consentement.

Lors de mes témoignages précédents devant le Comité, surtout au sujet des demandes de renseignements en vertu de la Loi sur la protection des renseignements personnels, on m'a posé des questions au sujet du droit à l'oubli et de sa pertinence pour le droit relatif au respect de la vie privée canadien. Mon opinion est toujours la même aujourd'hui: en règle générale, le droit à l'oubli n'est pas pertinent.

Depuis ce temps, la Cour fédérale du Canada a rendu sa décision dans l'affaire Globe24h.com qui, selon ce que je comprends, impliquait un Roumain qui gérait un site Web en Roumanie. Il fouillait les sites Web canadiens à la recherche des décisions des tribunaux et les publiait sur son site Web. La principale différence, c'est que les sites Web de ces tribunaux, gérés par des entités et organisations gouvernementales comme CanLII, mettent en place des mesures afin que le nom des personnes ne soit pas indexé dans les moteurs de recherche. Si vous êtes cité dans une affaire et que vous tapez votre nom dans un moteur de recherche, il n'apparaîtra pas dans ces bases de données.

L'intimé avait fait tomber cette protection ou ne l'avait pas appliquée. Une personne pouvait donc trouver son nom — qui était associé à une affaire — dans le moteur de recherche, ce qui pouvait être embarrassant, puisque pour la plupart des gens, l'expérience devant les tribunaux n'est pas très heureuse. Il avait par la suite mis en oeuvre un mécanisme permettant aux gens de faire une demande pour retirer leur nom. S'ils présentaient une demande par la poste, le délai de traitement était de six mois; s'ils faisaient un virement bancaire en ligne, on retirait leur nom immédiatement. Il s'agissait essentiellement d'une arnaque en matière d'extorsion.

Une personne dont les renseignements apparaissaient sur le site Globe24h.com a formulé une plainte au commissaire à la protection de la vie privée, qui a conclu que l'administrateur du site Web contrevenait au droit canadien en matière de protection de la vie privée — même si le site était en Roumanie et je crois que la décision n'avait pas trait à la compétence — et est passé à l'étape suivante, soit le renvoi à la Cour fédérale, comme le prévoit la LPRPDE. Dans sa décision, la Cour fédérale a fait valoir que les motifs — qui visaient l'extorsion — étaient déraisonnables et contrevenaient à la loi. La Cour a exigé que l'administrateur Web retire toutes ces décisions de son site — et, selon ce que je comprends, le site Web n'est plus actif — et qu'il verse une indemnité. Enfin, le tribunal a ordonné à cet homme, un Roumain, de ne plus mettre en ligne les décisions des tribunaux canadiens, puisque cela contrevenait à la loi.

Je souligne que cette décision — ou du moins cette affaire — n'a pas été contestée; il n'y avait donc aucune nuance relative à son interprétation ni aucune discussion sur les intérêts contraires, comme les droits relatifs à la liberté d'expression en vertu de l'alinéa 2b). La décision se fondait sur une disposition de la LPRPDE relative au journalisme qui a été jugée inconstitutionnelle dans un cas parallèle en Alberta; je ne crois donc pas qu'on puisse établir clairement que le droit à l'oubli se trouve dans la loi.

J'appelle à la prudence en ce qui concerne cette affaire, parce qu'elle n'a pas fait l'objet d'une contestation en soi, avant de conclure qu'elle injecte le droit à l'oubli dans la loi sur la protection de la vie privée existante. Je vous appelle aussi à la prudence si vous et d'autres intervenants songez à intégrer le droit à l'oubli à la loi sur la protection de la vie privée. Par exemple, en Europe, dans nombre des cas, la présence des renseignements sur Internet est tout à fait légale et l'indexation semble particulièrement problématique.

● (1630)

Dans les exemples donnés par Mme Vonn, si le contenu sous-jacent est diffamatoire, alors on peut obtenir une injonction pour le faire retirer. Est-ce que c'est en s'attaquant à l'indexeur qu'on réglera le problème?

Ce qui compte aussi, c'est que la Constitution et la Charte garantissent le droit à la liberté d'expression, mais nous n'avons pas un droit à la vie privée face aux entreprises. Ainsi, si l'on tente quoi que ce soit dans ce domaine, il faudra survivre à un examen fondé sur la Charte, ce qui sera difficile dans le contexte du droit à l'oubli.

J'aimerais maintenant parler des pouvoirs du commissaire à la protection de la vie privée. Selon mon expérience à titre de conseiller auprès des entreprises qui communiquent avec le commissaire à la protection de la vie privée de façon régulière, je ne crois pas que ce soit une bonne idée d'accroître les pouvoirs du commissaire. En fait, le commissaire a d'importants pouvoirs qui sont rarement utilisés. Si on lui conférait des pouvoirs exécutoires ou le pouvoir de percevoir des amendes auprès des organisations, ses nombreux rôles devraient faire l'objet d'un examen minutieux en vertu des principes de base de l'équité procédurale et de la justice fondamentale. Le commissaire défend bien entendu le droit à la vie privée. Il ne faudrait pas prendre à la légère l'octroi des pouvoirs de défenseur, d'autorité en matière d'éducation, d'enquêteur, de procureur et de juge à une personne ou une institution. En règle générale, ces fonctions sont distinctes, et il y a une raison à cela. On se retrouvera en situation de conflit d'intérêts si une même personne cible les malfaiteurs, enquête sur eux, les poursuit en justice, décide qu'ils sont des malfaiteurs et les punit. Ces pouvoirs sont distincts dans presque tous les cas. On se retrouverait avec une entité comme la Commission canadienne des droits de la personne, qui compte une commission et un tribunal. Je ne crois pas qu'on puisse défendre une telle structure institutionnelle pour offrir une justice rapide.

L'affaire Globe24h.com démontre toutefois la capacité du commissaire — et du plaignant — d'aller devant le tribunal. La LPRPDE prévoit un processus de demande accéléré. On peut comparaître devant un juge de la Cour fédérale et présenter son dossier. Le défendeur peut répondre, bien que dans le cas du Globe24h.com, il ait refusé de le faire. L'affaire est tranchée par un juge impartial qui peut ordonner à une organisation de changer ses pratiques. Il peut ordonner une indemnisation et des dommages-intérêts. Les dommages-intérêts peuvent être punitifs, mais vous remarquerez que ces pouvoirs visent presque tous des mesures de réparation, et je crois que c'est une bonne chose.

Ce qui m'inquiète aussi, c'est qu'en réorganisant le Commissariat à la protection de la vie privée, on perdrait l'esprit de collaboration et de coopération qui règne présentement. Si le commissaire à la protection de la vie privée est à la fois le policier et le procureur, les entreprises se prévaudront de leur droit au silence et ne collaboreront plus comme elles le font aujourd'hui. Selon mon expérience — il y a peut-être d'autres entreprises qui ne collaborent pas aussi bien que mes clients —, les clients souhaitent habituellement régler les choses; ils veulent négocier avec le commissaire. Pour ce faire, il faut un échange assez important, et une bonne collaboration. Si ce rôle change de façon drastique, alors on se retrouvera dans un tout nouvel environnement.

Enfin, et rapidement, au sujet du consentement, je crois que même si les technologies, les relations des personnes avec les technologies et la façon dont on recueille, on utilise et on communique les renseignements personnels sont beaucoup plus complexes qu'avant, l'abandon du principe du consentement est problématique.

Prenons par exemple la proposition de M. Geist au sujet du consentement volontaire. Je crois qu'il faut prendre un moment et songer à la façon dont cela se traduira dans de nombreuses circonstances. Par exemple, lorsque Twitter a été lancé, on offrait deux options: vos gazouillis pouvaient être publics ou privés. De nombreux défenseurs du droit à la vie privée font valoir que les paramètres par défaut de tout nouveau service, lorsqu'il est lancé, doivent offrir les plus hauts niveaux de protection. Cela aurait signifié qu'au jour un, lorsque vous vous seriez inscrits à Twitter, tous vos gazouillis auraient été protégés. Les premiers utilisateurs auraient crié dans une pièce vide. En fait, Twitter se voulait une plateforme publique pour les gens qui souhaitent s'exprimer publiquement. C'était l'objectif par défaut de Twitter, mais on pouvait restreindre ces paramètres.

Si une loi rendait la protection de vos gazouillis obligatoire ou si l'on devait appliquer la plus haute protection en matière de vie privée, alors Twitter aurait été lancé sans gazouillis protégés parce que le site aurait dû mettre en oeuvre cette mesure. Au bout du compte, la protection aurait été inférieure. Il faut faire preuve de prudence lorsqu'on prend de telles décisions, surtout en raison de la grande diversité des produits et services offerts.

J'hésiterais aussi à mettre en oeuvre un système qui empêcherait les personnes de faire un choix. L'une des valeurs fondamentales associées à la vie privée, c'est l'autonomie individuelle, ce qui est très bien. Certaines personnes ne voient aucun problème avec ces paramètres par défaut, qui les guident dans une certaine direction. Toutefois, les personnes qui prennent le temps de comprendre ou à qui l'on donne les moyens de comprendre ce qui se passe avec leurs renseignements personnels devraient avoir le droit de choisir.

● (1635)

Merci infiniment de m'avoir invité à participer à cette importante discussion. Je suis impatient d'entendre vos questions.

Le président: Merci beaucoup.

Nous allons maintenant entendre M. Bennett, s'il vous plaît, pour 10 minutes. Nous passerons ensuite immédiatement à la série de questions.

M. Colin Bennett (professeur, Secteur des sciences politiques, University of Victoria, à titre personnel): Merci, monsieur le président.

Merci de me donner l'occasion de comparaître à nouveau devant vous.

Je suis un professeur de sciences politiques à l'Université de Victoria, et je suis connu pour les travaux comparatifs que je fais sur la gouvernance en matière de protection de la vie privée dans les secteurs public et privé.

Je sais que vous aimeriez en savoir un peu plus sur la réglementation européenne et sur son incidence sur le Canada, alors c'est ce que je veux surtout aborder. Je vais peut-être aussi parler de la façon dont cette réglementation devrait influer ou non sur nos délibérations sur la LPRPDE. Je vais aussi mentionner trois secteurs où il y a des divergences flagrantes entre ce que nous faisons au Canada et ce que les Européens proposent.

Lorsque le règlement général sur la protection des données entrera en vigueur dans l'ensemble des pays de l'Union européenne en 2018, ce sera les exigences en matière de protection des données les plus exhaustives au monde qui, dans une grande mesure, établiront les normes relatives à la protection des renseignements personnels dans l'univers mondial du commerce électronique et de l'informatique en nuage. Pour des pays comme le Canada, ce règlement aura des répercussions extraterritoriales qu'il faudra examiner attentivement.

En vertu de la ligne directrice antérieure, comme vous le savez, le Canada a été jugé conforme aux normes européennes, c'est-à-dire que les entreprises pouvaient traiter légalement les données personnelles des citoyens européens sans mécanismes contractuels. L'Union européenne n'estimait pas que le Canada se conformait à ses normes et considérait seulement les organismes assujettis à la LPRPDE comme ayant le caractère adéquat. Néanmoins, le caractère adéquat offrait des avantages pratiques importants aux entreprises canadiennes. Plus important encore, il transmettait le message symbolique selon lequel le Canada était un pays sécuritaire où les données personnelles pouvaient être traitées. Cette question revêt bien entendu une plus grande importance dans le cadre de l'AECG, qui accroîtra probablement les échanges commerciaux et les quantités de données personnelles des consommateurs et des employés qui sont transmises au Canada.

Jusqu'à présent, seulement 11 pays ont été jugés comme étant conformes aux normes européennes, et le Canada est de loin l'économie la plus importante parmi eux. Pour les États-Unis, le caractère adéquat est accordé seulement aux entreprises qui se sont autocertifiées en vertu du nouveau bouclier de protection entre l'Union européenne et les États-Unis. Conformément au règlement général sur la protection des données, le caractère adéquat sera maintenu, et les pays qui auront reçu ce statut continueront de tirer parti des avantages qu'il offre. La Commission européenne envisage d'adopter un mécanisme d'examens périodiques tous les quatre ans. Nous pouvons donc nous attendre à ce qu'une évaluation canadienne soit menée d'ici 2021, mais il n'y a aucune garantie que ce statut continuera d'offrir ces avantages. De plus, il y a de nombreux autres pays qui veulent probablement obtenir le statut. La différence entre la situation en 2001 et maintenant, c'est qu'il y a près d'une centaine de pays dans le monde qui ont des lois sur la protection des données qui s'apparentent au modèle européen.

En octobre 2015, la Cour européenne de justice a rendu une décision dans l'affaire Schrems portant sur Facebook, qui a invalidé l'accord Safe Harbor entre l'Union européenne et les États-Unis et qui a changé les politiques sur l'évaluation du caractère adéquat de bien des façons. Il y a trois points à souligner.

Premièrement, une décision existante relative au caractère adéquat ne soustrait pas une autorité européenne de protection des renseignements personnels à la responsabilité de mener une enquête sur une plainte déposée contre une entreprise située dans un autre pays. Le caractère adéquat n'est pas, et n'a probablement jamais été, une échappatoire. Les entreprises canadiennes sont aussi vulnérables que d'autres de faire l'objet de poursuites dans l'Union européenne.

Deuxièmement — et plus récemment depuis les révélations de Snowden —, toute la question de l'accès aux données des entreprises par les services de sécurité et du renseignement est maintenant très importante pour déterminer le caractère adéquat d'une entité. En 2013, la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen a réclamé la tenue d'un examen du régime de protection des renseignements personnels du Canada, à la lumière de notre participation au Groupe des cinq. Cette question fait donc maintenant partie du processus d'évaluation. Ces préoccupations doivent également être examinées à la lumière des garanties fournies par le gouvernement américain dans le cadre du bouclier de protection entre l'Union européenne et les États-Unis selon lesquelles l'accès aux données personnelles par les organismes américains d'application de la loi et de sécurité nationale sera assujetti à des restrictions et à des mesures de protection et de surveillance, même si elles seront passées en revue et font l'objet d'un litige en Europe actuellement.

● (1640)

Troisièmement, la Cour européenne a relevé la barre pour les évaluations du caractère adéquat pour avoir ce que l'on appelle l'« équivalence essentielle ». Nous n'avons pas d'indications claires quant à savoir ce que cela signifie. C'est un peu comme réviser pour un examen sans connaître les normes de notation. Quels aspects de la protection des renseignements personnels seront considérés comme étant essentiels? Il y a de nouveaux éléments dans le règlement sur la protection des renseignements personnels qui ne figuraient pas dans la directive et qui ne sont pas très importants dans la LPRPDE non plus. Feront-ils partie du critère? Mes collègues ont discuté du droit à l'oubli. Il y a un droit relatif à la portabilité des données prévu dans le règlement, ce dont je pourrais parler. Il y a le droit de contester des décisions prises concernant le traitement automatisé. Il y a la protection de la vie privée dès la conception et la protection par défaut. Quels sont les principes essentiels et quelles sont les méthodes d'application de la loi et de mise en oeuvre?

Pour l'instant, les exigences relatives au caractère adéquat prévues dans le règlement sont très vagues. Elles doivent être appliquées avec cohérence, et je présume que l'Union européenne n'insistera pas pour que d'autres pays, surtout les États-Unis, procèdent à des réformes juridiques qui sont irréalistes sur le plan politique ou qui présenteront des problèmes constitutionnels. Ainsi donc, je pense que nous devrions hésiter à réviser la LPRPDE pour la simple raison que les Européens veulent que nous le fassions. Quoi qu'il en soit, il y a des propos inutiles qui sont tenus selon lesquels ce règlement est un modèle d'excellence en matière de protection des renseignements personnels dans le monde. C'est une combinaison de différentes dispositions, dont certaines ont été importées de pays comme le Canada. Nous devrions moderniser la LPRPDE car elle a besoin d'être mise à jour, et non pas parce qu'elle respecte un ensemble de normes vagues et changeantes imposées par Bruxelles. Nous devrions prendre note que les Européens ont tiré des leçons. Je crois que des efforts importants pour mettre à jour et modifier la LPRPDE ne passeront pas inaperçus de l'autre côté de l'Atlantique. En revanche, j'estime que le fait de laisser la loi dans sa forme actuelle enverrait le mauvais message.

Pour terminer, j'aimerais attirer votre attention sur trois grands secteurs où, à mon avis, il y a les divergences les plus flagrantes entre ce que fait la LPRPDE et ce que le règlement européen prévoit.

Premièrement — et je ne vais pas aborder ce point parce mes collègues en ont parlé —, il y a les pouvoirs d'application de la loi du commissaire à la protection de la vie privée. En vertu du règlement général sur la protection des données, les agents de protection des données ont le pouvoir d'imposer des amendes administratives très importantes aux entreprises — pouvant s'élever jusqu'à 20 millions d'euros ou 4 % de leur chiffre d'affaires annuel. À mon avis, nous ne devrions pas être aussi sévères. Les amendes rendent l'intention de la loi comme aucune autre sanction, mais de façon générale, et j'ai réfléchi à la question, je pense que le commissaire à la protection de la vie privée devrait à tout le moins avoir les mêmes pouvoirs que ceux dont dispose le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique en vertu de notre loi applicable au secteur privé.

Deuxièmement, nous devons nous assurer que le commissaire à la protection de la vie privée dispose de tous les outils disponibles en matière de protection des renseignements personnels. À l'heure actuelle, la LPRPDE est rédigée d'une façon très réactive. La loi est rédigée comme si l'intégralité de ces travaux sont consacrés aux enquêtes sur les plaintes et au règlement des plaintes. Comme David Fraser l'a dit, il y a des dispositions dans la LPRPDE qui n'ont pas été utilisées activement au fil des ans. Je crois que les fonctions les plus efficaces sont plus proactives et comprennent une variété d'autres instruments. À mesure que le consentement personnel devient beaucoup plus difficile à obtenir dans cette ère d'analyse des mégadonnées, je pense que les organismes devront se fier à ces autres outils. Le règlement général sur la protection des données et d'autres lois modernes sur la protection des renseignements personnels reconnaissent l'importance de ces autres instruments stratégiques dans l'application de la loi et la mise en oeuvre efficaces. Ils stipulent que les organismes doivent se tenir prêts à démontrer qu'ils respectent ces mesures législatives en utilisant des mécanismes comme des codes de pratique, des sceaux de protection, des normes et des évaluations des facteurs relatifs à la vie privée. Le règlement essaie d'encourager de bonnes pratiques de protection de la vie privée, et je crois que la LPRPDE devrait essayer de faire la même chose.

J'aimerais donc qu'il soit expressément reconnu à l'article 24 de la LPRPDE que le commissaire peut encourager l'utilisation de ce type d'outils et, dans certains cas, oblige l'adoption de ces mécanismes de reddition de comptes par les entreprises canadiennes et leurs associations commerciales. Plus particulièrement, il y a la protection de la vie privée dès la conception et la protection par défaut.

● (1645)

Le règlement général sur la protection des données prévoit que les organismes devraient, dans la mesure du possible, s'assurer que les données personnelles qui sont traitées sont seulement celles qui doivent absolument l'être. C'est complexe. Le règlement veille à ce que la protection des renseignements personnels fasse partie intégrante du développement technologique et de la structure organisationnelle de tout nouveau produit et service. Lorsque les organismes ne respectent pas cette exigence, ils sont passibles de sanctions sévères si des enquêtes sont menées.

Le vice-président (M. Nathaniel Erskine-Smith (Beaches—East York, Lib.)): Monsieur Bennett, je ne veux pas vous interrompre, mais nous avons dépassé les 10 minutes et il nous restera probablement moins d'une demi-heure pour la période des questions. Si vous pouviez conclure vos remarques, ce serait apprécié.

M. Colin Bennett: J'allais discuter des évaluations des facteurs relatifs à la vie privée, des codes de pratiques, des normes et de la certification, ainsi que du traitement des données sensibles. Il y a une énorme différence entre ce qui est prévu dans la LPRPDE et le règlement au sujet des données sensibles. Plus particulièrement, je pense qu'il y a une différence, comme Micheal Vonn l'a dit, relativement au traitement des données sur les opinions et les affiliations politiques.

Je vous remercie infiniment de l'attention que vous m'avez accordée. Je suis désolé d'avoir dépassé légèrement le temps qui m'a été imparti. Je me ferai un plaisir de répondre à vos questions.

Le vice-président (M. Nathaniel Erskine-Smith): Merci beaucoup à tous les témoins.

Nous allons commencer avec M. Saini.

M. Raj Saini (Kitchener-Centre, Lib.): Merci à vous tous d'être ici aujourd'hui. Je reconnais certains d'entre vous, car vous avez déjà comparu ici dans le passé.

Vous avez tous fait allusion aujourd'hui au droit à l'oubli.

Je vais commencer avec vous, monsieur Fraser, car vous avez rédigé des notes très claires sur la question. Vous avez dit qu'il serait improbable de pouvoir résister à une contestation fondée sur la Charte à moins que ce soit une question pressante ou importante.

J'ai une question pour vous. Avec l'arrivée des médias sociaux notamment, il y a des enfants qui utilisent les médias sociaux, des mineurs plus particulièrement. D'après vous, devrait-il y avoir des dispositions pour les protéger ou pour leur permettre de se prévaloir du droit à l'oubli, surtout lorsqu'ils ont moins de 14 ou de 16 ans, d'une certaine limite d'âge arbitraire? S'ils font quelque chose durant leur enfance, devraient-ils en être tenus responsables?

J'aimerais entendre l'opinion de tous les témoins, mais j'aimerais commencer avec vous.

M. David Fraser: D'accord. Je pense qu'une partie de ce que nous croyons être le droit à l'oubli ou le droit à l'effacement, comme on l'appelle en Europe récemment, existe vraiment. Vous avez la capacité de révoquer le consentement que vous avez déjà donné. Le commissaire à la protection de la vie privée a fait une enquête sur la fermeture de comptes sur Facebook, et tout cela existe.

Donc, dans le cas de toute organisation commerciale qui recueille, utilise ou communique ces renseignements, le consentement peut être révoqué et vous pouvez exiger que ces renseignements soient supprimés.

● (1650)

M. Raj Saini: Monsieur Geist.

M. Michael Geist: Vous avez mentionné si des mesures de protection devraient ou non être en place pour les mineurs, et il convient de signaler que ces mesures existent aux États-Unis. Ils ont fixé des lois de protection des renseignements personnels plus sévères, surtout pour les jeunes de 13 ans et moins. Il y a un débat raisonnable sur l'efficacité de ces règles, mais on a reconnu que les jeunes doivent être mieux protégés.

Je dirais que quelques-unes des recommandations que j'ai faites et que le Comité a entendues d'autres témoins contribueraient grandement à offrir ces mesures de protection. Je connais David depuis longtemps et je le respecte beaucoup, mais l'idée qu'une norme facultative fasse disparaître la possibilité de choisir me paraît complètement contraire à ce qu'elle fait. Une approche facultative permet de faire des choix. Les choix sont ainsi mieux éclairés. Donc, le défi est en partie, pour les mineurs et pour bien d'autres, de veiller à ce qu'ils aient l'éducation et les outils nécessaires pour faire des choix éclairés concernant leur vie privée. S'il y a un problème, bien souvent, ce sont les entreprises qui profitent des gens qui ignorent l'utilisation qu'elles feront de leurs renseignements personnels. Cela peut être particulièrement vrai chez les enfants qui subissent souvent des pressions par leurs pairs pour afficher des renseignements et n'ont pas bien réfléchi aux choix à faire concernant leur vie privée.

Je pense qu'un modèle fondé sur le consentement plus rigoureux contribuerait grandement à régler une partie du problème.

M. Raj Saini: Madame Vonn.

Mme Micheal Vonn: Oui, merci.

En ce qui concerne l'idée de révoquer le consentement aux entreprises privées, on ne peut pas vraiment le faire une fois que les renseignements sont dispersés sur Internet. Il faut donc absolument examiner le potentiel, dans les circonstances appropriées — où il n'y a pas de droits compensatoires qui briment le droit à la liberté d'expression notamment, et où il n'est pas question de personnalité publique, mais d'une personne ordinaire —, pour supprimer le lien... une fois que les renseignements sont disséminés en ligne. Vous n'avez pas l'option de communiquer avec le fournisseur de services, car cela dépasse son mandat. Vous ne pouvez pas révoquer le consentement.

M. Raj Saini: Merci de cette réponse.

Monsieur Bennett, je ne veux pas que vous vous sentiez oublié. Je vais vous poser une question d'ordre international puisque vous avez soulevé le RGPD.

Maintenant que nous avons signé l'AECG, nous avons maintenant à l'interne la question des barrières au commerce entre les provinces. Trois provinces n'ont pas adopté la LPRPDE, qui est considérée comme étant très semblable aux lois existantes en Colombie-Britannique, au Québec et en Alberta. Nous avons un problème au pays car il n'y a pas d'uniformité, mais nous avons maintenant signé l'AECG, et je suis certain que dans l'avenir, nous signerons d'autres accords de libre-échange — et vous avez mentionné le bouclier de protection des données entre l'Union européenne et les États-Unis. À mon sens, il semble y avoir deux ou trois normes différentes, que ce soit le RGPD, le bouclier de protection des données de l'Union européenne ou notre participation au Groupe des cinq.

Y a-t-il un moyen de moderniser et de normaliser notre régime de protection des renseignements personnels, pas seulement à l'échelle nationale mais aussi à l'échelle internationale, pour que nos partenaires commerciaux internationaux le comprennent et que nous puissions avoir un seul régime au pays plutôt que deux ou trois?

● (1655)

M. Colin Bennett: C'est ce que je souhaite.

Sur le sujet des lois provinciales, je pense que l'on supposait au départ que si la LPRP en Colombie-Britannique et en Alberta et la loi au Québec étaient considérées comme étant très semblables à la LPRPDE, elles seraient considérées, par défaut, adéquates en vertu des normes de l'Union européenne. L'Union européenne a toutefois rejeté une demande indépendante du Québec visant à déclarer sa loi adéquate, si bien que cette supposition n'est pas tout à fait correcte. C'est une question qu'il faudra régler dans le cadre de l'examen à venir du caractère adéquat du Canada conformément au RGPD de l'Union européenne.

À l'heure actuelle, des normes relatives au caractère adéquat de l'Union européenne existent, mais sont très vagues. Elles portent sur le respect de votre loi. Elles portent sur les principes essentiels de la protection des données. Elles portent sur l'existence de mécanismes de recours. Elles établissent la distinction très subtile entre la protection des droits des citoyens européens lorsque leurs renseignements personnels sont traités à l'étranger et l'ingérence dans les politiques et les exigences constitutionnelles d'autres pays. C'est là où la tension règne aux États-Unis.

En ce qui concerne le bouclier de protection des données entre l'Union européenne et les États-Unis, je pense que le maintien de cet accord est incertain à l'heure actuelle, pour plusieurs raisons. Premièrement, la norme qui a été négociée était l'ancienne directive européenne et non pas la nouvelle. Deuxièmement, il y a un litige en Europe en ce moment, surtout en Irlande, concernant les mécanismes utilisés par Facebook pour transférer des données aux États-Unis. Des deux côtés de l'Atlantique, on pourrait mettre fin à cet accord.

Quant à savoir si l'on devrait en tenir compte ou non, je ne pourrais pas vous dire, car nous ne savons pas ce que l'avenir nous réserve.

Le président: Merci beaucoup, monsieur Saini.

Nous allons maintenant passer à M. Kelly. Je crois qu'il partagera son temps avec M. Jeneroux, s'il en reste.

Monsieur Kelly, vous avez jusqu'à sept minutes.

M. Pat Kelly: Nous verrons comment cela se passe.

Si je peux me permettre, j'aimerais commencer par poser à M. Geist des questions sur la localisation des données.

Vous avez donné certains détails à ce sujet et vous avez dit certaines choses qui m'ont intrigué et que j'aimerais approfondir.

Si j'ai bien compris, vous avez dit que la localisation est importante pour les Canadiens. Vous avez nommé de grands responsables de la collecte de données et affirmé qu'il est nécessaire ou souhaitable d'avoir des données localisées au Canada, tout en reconnaissant que la localisation des données n'est pas souhaitable dans des pays — vous avez nommé la Chine — où les restrictions relatives à la transmission posent problème et sont contrôlées par l'État.

Certains de nos autres partenaires internationaux pourraient-ils s'opposer à ce que le Canada se considère le juge des endroits où la localisation est bonne ou mauvaise? À votre avis, qu'en pensera la communauté internationale?

M. Michael Geist: Merci de poser la question. Je vais décortiquer un peu tout cela. Dans une certaine mesure, vous avez parlé du transfert des données et de la localisation des données, qui sont deux choses différentes.

La localisation des données est une réalité des pays qui exigent aux entreprises de stocker ou de conserver localement les renseignements personnels, s'assurant ainsi que ces renseignements bénéficient des protections offertes par la législation nationale. À vrai dire, c'est également ce que notre gouvernement national fait dans le cadre d'une stratégie d'informatique en nuage enclenchée par les conservateurs et poursuivie par les libéraux. Il reconnaît ainsi que nous ne voulons pas que certains renseignements détenus par le gouvernement soient stockés sur des serveurs à l'étranger.

À mon avis, ce que nous verrons probablement dans l'ALENA et ce que nous avons vu dans le PTP — en grande partie à la demande des États-Unis qui représentent certaines des entreprises qui ont tendance à stocker de grandes quantités de données et à le faire au sud de la frontière —, ce sont des tentatives visant à empêcher des pays de se donner le mandat d'exiger que les données soient stockées localement. Nous voyons certainement certains efforts déployés en ce sens par les entreprises.

C'est pourquoi ces grandes entreprises ont des serveurs au Canada. En un sens, elles répondent à la demande du marché, dans lequel on veut une meilleure protection, mais je dirais que le Canada devrait certainement être libre de dire que nous voulons nous assurer de conserver certains types de renseignements au pays pour que les Canadiens sachent que ces renseignements sont protégés adéquatement et assujettis aux règles canadiennes. Je crains qu'il soit possible que l'on tente de se soustraire à cette restriction dans le cadre des négociations commerciales.

Je signale rapidement que c'est différent des restrictions visant le transfert de données à la frontière. Nous avons également observé que les États-Unis s'emploient à mettre fin à ces restrictions, mais comme vient tout juste de l'expliquer M. Bennett, c'est exactement ce que l'Union européenne a essayé de faire, à savoir restreindre la capacité de transférer des données à certaines frontières.

M. Pat Kelly: La facilité du transfert se traduit toutefois par une localisation différente, un lieu de stockage différent. S'il est facile de transférer des données à l'étranger, on peut les stocker ailleurs. N'est-ce pas ce que...

M. Michael Geist: Il y a deux choses à retenir. Tout d'abord, il est toujours facile de transférer des données. Si on tient seulement compte de la facilité du transfert, on devrait alors craindre que les données se retrouvent dans le pays ayant la plus faible protection. Je ne pense pas que beaucoup de Canadiens se sentiraient à l'aise si on leur disait qu'une grande partie des protections qu'ils croient avoir sont perdues parce que leurs données sont stockées dans un pays où les renseignements personnels ne sont aucunement protégés, et il serait très difficile pour un commissaire à la protection de la vie privée de faire respecter notre souveraineté.

Même dans le contexte du transfert des données, ce que nous voyons souvent au Canada, c'est qu'un courriel envoyé par quelqu'un ayant un fournisseur comme Bell ou Rogers peut passer par les États-Unis et revenir au Canada. Par conséquent, même la question de permettre aux données de traverser la frontière — j'admets que c'est facile à faire — est considérée par certains pays comme une source d'inquiétudes.

Je voulais surtout signaler ce problème de localisation étant donné que nous avons vu des entreprises déployer des efforts soutenus pour se soustraire aux restrictions. Nous avons également entendu les gens du gouvernement du Canada en parler, et le terme commence à faire partie du vocabulaire des négociations commerciales. Compte tenu de ce que nous avons entendu de la part de l'administration Trump, il semble fort probable que la question soit abordée de nouveau dans le cadre de la renégociation de l'ALENA.

● (1700)

M. Pat Kelly: Merci.

Dans ses observations sur l'affaire roumaine d'extorsion, M. Fraser m'a fait penser à la question de la localisation, à la facilité du transfert ainsi qu'au lien entre les deux. Je vous demanderais d'intervenir si vous voulez parler du niveau de compréhension, d'adoption et de respect de la LPRPDE dans sa forme actuelle. Vous êtes nombreux à avoir parlé du bien-fondé des peines sévères pour encourager le respect de la loi. Comme j'ai fait carrière dans une petite entreprise, je sais qu'on sensibilise beaucoup les propriétaires d'entreprise à la Loi sur les renseignements personnels, qu'ils veulent s'y conformer et qu'ils craignent les conséquences du non-respect de la loi. Sinon, on comprend très peu ce que tout cela signifie.

Si vous avez des observations à faire à ce sujet, allez-y.

M. David Fraser: Je pratique tous les jours le droit à la vie privée en donnant des conseils aux entreprises, et je crois qu'il convient de signaler une chose — c'est sans aucun doute ce que j'ai vu et entendu —, à savoir que les grandes banques, les grandes entreprises de télécommunications emploient des escadrons d'avocats. Ils ont du personnel qui se consacre à la conformité, à la conformité à l'échelle internationale. En fait, leur niveau de conformité est très élevé, mais leur seuil de risque diffère peut-être un peu de celui d'une PME.

Leur compréhension des rouages du respect de la législation canadienne en matière de protection des renseignements personnels — comment obtenir le consentement des gens, gérer le tout et protéger les renseignements — est plutôt limitée dans la plus grande partie de notre économie. Je parle ici de l'ensemble des PME.

Je crois qu'il vaut la peine de mentionner — et je n'ai pas de solution facile — que même si le commissaire à la protection de la vie privée a fait beaucoup de travail auprès des grandes banques, des grandes entreprises de télécommunications et des fournisseurs de services Internet, il faut se demander comment sensibiliser et approcher ces PME et les inciter à mieux protéger les renseignements personnels des Canadiens. Je n'ai pas de solution toute prête.

Le président: Merci beaucoup, monsieur Kelly.

Nous passons maintenant à M. Blaikie.

M. Daniel Blaikie (Elmwood—Transcona, NPD): Merci beaucoup.

J'aimerais reprendre notre discussion sur nos partenaires internationaux et la mesure dans laquelle la législation canadienne en matière de protection des renseignements personnels est dictée par un accord commercial ou notre souhait de pouvoir transférer facilement l'information, comme c'est le cas en Europe. L'AECG nous a vraisemblablement donné l'occasion d'avoir une protection supplémentaire — en faisant reconnaître de manière plus officielle les pratiques canadiennes en matière de protection des renseignements personnels pour qu'elles soient moins incertaines. Nous semblons toutefois avoir raté cette occasion.

À mesure que la technologie et la négociation d'accords commerciaux progressent, à quel point vous attendez-vous à ce que ces questions soient tranchées par des partenaires commerciaux internationaux plutôt que par des législateurs canadiens? Quelle est l'interaction entre la législation canadienne et les accords commerciaux?

M. Michael Geist: Je vais essayer de répondre. Michael, Colin et David ont sans aucun doute des réponses.

Je dirais rapidement qu'il est évident que ces questions font maintenant partie des négociations commerciales. Nous l'avons assurément vu pour ce qui est du Partenariat transpacifique, le PTP. Par ailleurs, le secrétaire au Commerce des États-Unis, Wilbur Ross, a parlé de la nécessité de discuter de l'économie numérique dans le cadre de la renégociation de l'ALENA.

Dans le chapitre du PTP sur le commerce électronique, on voit les grandes lignes des questions susceptibles d'être soulevées dans la renégociation de l'ALENA. Elles portent sur des choses comme la localisation et le transfert des données. Je signale que le PTP comportait également une disposition selon laquelle les pays devaient avoir une législation en matière de protection des renseignements personnels, mais c'était une version très édulcorée étant donné que les États-Unis n'ont pas de règles de portée générale en la matière, malgré une application rigoureuse.

Je pense qu'il ne fait aucun doute que nous continuerons de subir des pressions, ce qui pourrait être une bonne chose dans certains cas. David a dit à quoi ressemblerait un cadre législatif dans lequel le commissaire à la protection de la vie privée aurait le pouvoir de rendre des ordonnances. Il a laissé entendre que cela ressemblerait à la commission des droits de la personne. Je dirais que cela ressemblerait au cadre sur la protection des renseignements personnels d'à peu près tout le monde. Les pouvoirs du commissaire seraient semblables à ceux des commissaires des provinces. Cela s'apparenterait davantage à ce qu'on voit dans l'Union européenne, même à ce qu'on voit à la Commission fédérale du commerce des États-Unis, où le commissaire a le pouvoir de rendre des ordonnances et de faire respecter l'approche commune dans beaucoup d'autres endroits. Dans ce cas-ci, l'exception est le commissaire fédéral à la protection de la vie privée, qui ne détient pas ce pouvoir.

● (1705)

M. Daniel Blaikie: Quelqu'un d'autre souhaite-t-il intervenir?

M. Colin Bennett: Je suis d'accord.

J'ajouterais juste un autre aspect. C'est une chose dont j'ai parlé très brièvement. Dans la politique de l'évaluation du caractère adéquat, c'est un jugement politique, pas un jugement juridique. J'ai quelques points à faire valoir à ce sujet. Le premier est que les Européens veulent vraiment que ce système fonctionne; ils ne veulent pas que le processus de l'évaluation du caractère adéquat disparaisse. Par conséquent, je pense qu'il y aurait un coût si, comme je le dis, un pays comme le Canada, un partenaire commercial, perdait son statut en matière de protection adéquate.

Deuxièmement, je tiens seulement à répéter que toute la question de l'accès des services de renseignement, des services de sécurité nationale et ainsi de suite à des données liées aux entreprises fait également partie de l'équation. Prenons l'accord de bouclier de protection conclu entre l'Union européenne et les États-Unis. On voit que cette question y occupe autant de place que les transferts commerciaux.

M. Daniel Blaikie: L'une des choses que nous avons entendues au sujet de la LPRPDE est qu'elle contient un énoncé général des principes. Pensez-vous que c'est logique... Il me semble qu'il ne serait pas acceptable que le droit à la vie privée des Canadiens figure constamment à l'ordre du jour chaque fois que nous entamons des négociations commerciales. On pourrait finir par échanger le droit à la vie privée des Canadiens contre une chose qui n'a rien à voir avec ce droit, comme le prix du riz ou quelque chose d'autre. Savez-vous ce que cela signifie?

Certaines choses ne doivent pas être cédées hâtivement, car elles sont totalement différentes. Je m'excuse de ne pas avoir les connaissances juridiques nécessaires. Pour ce qui est d'inscrire des principes dans la loi, si le commerce international continue d'être un aspect important de l'établissement du droit à la vie privée des Canadiens, ne serait-il pas logique d'avoir quelque chose comme un énoncé dans la LPRPDE pour indiquer que le gouvernement doit chercher à défendre le droit à la vie privée des Canadiens dans le cadre des négociations commerciales, ou qu'il doit chercher à incorporer les principes de la LPRPDE dans les accords commerciaux? Cette façon de procéder serait-elle logique et préférable à ne pas savoir si un ministère qui négocie un accord commercial se préoccupe du mandat d'autres ministères chargés de protéger les renseignements personnels des Canadiens.

M. Michael Geist: Je pense que les principes généraux nous sont très utiles, mais ce que nous voyons, notamment depuis l'arrivée des nouvelles technologies ces dernières années, ce sont des mesures législatives ou des règlements qui tentent d'encadrer les nouvelles préoccupations, qu'il s'agisse du vol d'identité, des pourriels ou de nouvelles questions de sécurité nationale. Il est maintenant probable que nous verrons surgir certaines de ces nouvelles préoccupations. Nous avons même vu la localisation des données être mentionnée à l'échelle provinciale dans un certain nombre de cas.

Je pense qu'il faut entre autres se tenir au fait de la situation. Dans le cas du PTP, nous voyons que les Australiens savaient exactement de quoi je parle. Ils ont obtenu une lettre d'entente des États-Unis qui portait précisément sur le risque qu'ils soient assujettis d'une part aux demandes de l'Union européenne et, d'autre part, aux demandes des États-Unis dans le cadre du PTP. Avec tout le respect, les législateurs canadiens semblaient dormir au volant et n'ont pas soulevé le même genre de questions et obtenu le même genre de choses. Si le PTP — qui semble maintenant chose du passé — s'était concrétisé, l'Australie aurait bénéficié d'une protection relative au transfert des données et aux renseignements personnels, contrairement au Canada.

M. Daniel Blaikie: Nous ne nous attendons habituellement pas — malgré la taille importante et la grande expertise des équipes de négociations commerciales — à ce que les négociateurs soient capables de tout prévoir lorsque nous approfondissons une question en tant que comité ou dans divers ministères.

Si les accords commerciaux ont un effet déterminant sur un type particulier de protections, est-il logique d'inscrire quelque part dans les principes d'une loi régissant ces protections pour les Canadiens que c'est un objectif du gouvernement du Canada d'essayer d'intégrer les mêmes protections dans les accords internationaux? Ce n'est évidemment pas contraignant. Cela ne veut pas dire qu'on ne peut pas signer d'entente. Il y aura toujours des compromis, mais il faudrait que ce soit inscrit dans une loi pour que les équipes canadiennes de négociation soient plus susceptibles d'en tenir compte. Cette inscription leur signalerait qu'elles doivent aborder la question dans le cadre des négociations.

Est-il logique d'essayer d'y accorder de l'attention en tant qu'outil?

M. Michael Geist: Ce qui serait logique, c'est que le Canada améliore la transparence des négociations commerciales. S'il y avait un problème fondamental dans la façon dont le gouvernement conservateur — avec tout le respect — a négocié l'AECG et le PTP, c'est le profond secret qui entourait les négociations et la façon dont il a ensuite dit que c'était à prendre ou à laisser.

Le PTP est chose du passé. L'ACTA, qui faisait partie des négociations, est lui aussi chose du passé, et des questions clés de l'AECG ont dû être renégociées en grande partie par les libéraux à cause du secret ayant entouré les négociations. Pour éviter qu'une telle situation se reproduise dans le cadre de la renégociation de l'ALENA, il faut faire preuve d'une plus grande transparence. La solution n'est pas de s'assurer que tous les négociateurs connaissent les nuances de chaque dossier, mais plutôt de faire participer au processus un grand nombre d'experts pour que ces questions soient signalées pendant les négociations — pas après coup lorsqu'il est trop tard pour agir.

● (1710)

Le président: Merci beaucoup.

Monsieur Erskine-Smith, vous avez sept minutes.

Chers collègues, nous arrivons maintenant au point où le timbre se fera entendre. Je présume que nous laisserons M. Erskine-Smith tirer parti des sept minutes à sa disposition.

Je vais devoir obtenir le consentement unanime du Comité pour poursuivre si le timbre se fait entendre. Avons-nous le consentement unanime pour continuer si nous le désirons? Les votes ne commenceront pas avant 17 h 45. Ou préféreriez-vous laisser M. Erskine-Smith terminer son intervention?

M. Daniel Blaikie: Voulez-vous obtenir le consentement unanime pour le laisser finir son intervention de sept minutes ou pour continuer indéfiniment après avoir entendu le timbre?

Le président: Je vais le laisser finir son intervention de sept minutes. Je veux avoir du temps par la suite.

M. Daniel Blaikie: Je pense que nous devrions terminer par...

Le président: Bien. Nous allons terminer par les questions de M. Erskine-Smith. Allez-y.

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

Je vais commencer par vous, monsieur Fraser. Vous avez remis en doute ou formulé une mise en garde concernant notre suggestion d'accorder de nouveaux pouvoirs au commissaire. Vous avez également parlé de l'équité procédurale, et je veux donc savoir ce que vous en pensez.

Si j'ai bien compris, certains organismes ont déjà le pouvoir d'imposer des sanctions administratives pécuniaires, par exemple le CANAFE; le CRTC en ce qui a trait à la loi antipourriel; le commissariat à l'éthique; et le commissariat à l'information du Royaume-Uni, qui, en 2013, a imposé à Sony une amende de 250 000 $ à la suite d'une violation relative au PlayStation. Ces modèles vont-ils tous à l'encontre de l'équité procédurale? Ces organismes font-ils face aux mêmes obstacles que vous avez mentionnés?

M. David Fraser: Je pense que toutes ces entités se trouvent devant les mêmes questions et font l'objet d'une surveillance semblable, et que bon nombre d'entre elles ont abordé ces enjeux de diverses manières afin d'incorporer ce volet. Beaucoup se sont dotées de pare-feu précis pour éviter que leurs enquêtes ne soient contaminées par leurs activités de promotion.

Ce que je dis, c'est que si vous voulez installer un véritable pare-feu d'envergure, celui-ci finirait par ressembler à la Commission canadienne des droits de la personne ou à d'autres modèles.

M. Nathaniel Erskine-Smith: J'aimerais toutefois revenir quelque peu en arrière: est-ce que cela ressemble à la position du commissaire à l'information du Royaume-Uni? C'est peut-être le cas, mais je connais moins bien cette réalité. Mais si ce commissaire a pu imposer une amende de 250 000 $, voilà qui m'apparaît plus efficace que les pouvoirs actuels de notre propre commissaire.

Si vous ne partagez pas cet avis, pouvez-vous nous dire le problème que posent les pouvoirs du commissaire du Royaume-Uni et ce genre de modèle? Vous ne les connaissez peut-être pas bien.

M. David Fraser: Non, je ne connais pas assez bien la structure du commissariat du Royaume-Uni.

M. Nathaniel Erskine-Smith: Très bien.

Vous avez parlé de dommages et intérêts relatifs aux articles 14 et 16 de la LPRPDE, de la façon dont ils se positionnent l'un par rapport à l'autre. Pensez-vous que les dommages et intérêts sont des mesures de dissuasion suffisantes? J'aimerais simplement mentionner que la dernière affaire dont je me souvienne vraiment de l'époque où j'étais étudiant en droit, c'est l'arrêt Ward et les 5 000 $ en dommages et intérêts qui ont été accordés pour une fouille à nu illégale. Le montant m'avait semblé dérisoire pour une grave atteinte à la vie privée. Par conséquent, trouvez-vous que les dommages et intérêts sont suffisants?

M. David Fraser: Peut-être qu'il faudrait notamment se demander s'il est convenable qu'une seule personne puisse s'adresser aux tribunaux pour une plainte donnée. Mais la mesure se veut une forme d'indemnisation, et dans ce cas-ci, un juge indépendant a déterminé qu'une somme de 5 000 $ était suffisante, à la lumière de tous les éléments de preuves devant lui.

Selon la Cour d'appel de l'Ontario, les dommages-intérêts généraux qui peuvent être imposés lorsque les sentiments sont heurtés relativement à une atteinte à la vie privée varient entre une valeur nominale et une somme de 20 000 $. Ces dommages et intérêts ont été prévus par notre système juridique, et je n'ai pas bien des raisons de les remettre en question.

M. Nathaniel Erskine-Smith: Les recours visent soit l'indemnisation, soit la dissuasion. Lorsque nous examinons nos recommandations sur les nouveaux pouvoirs du commissaire à la protection de la vie privée, il me semble qu'une plus grande dissuasion est peut-être nécessaire.

Vous avez exprimé des réserves au sujet du modèle de consentement actif que M. Geist a proposé. Lorsque le commissaire à la protection de la vie privée a comparu devant nous, il a parlé du consentement valable. Si nous ne choisissons pas le modèle de consentement actif, comment pourrions-nous améliorer le modèle en place de façon à obtenir un consentement valable?

M. David Fraser: À vrai dire, il y a peut-être un peu de confusion. Il a été question de protection de la vie privée par défaut, où l'élément le plus protégé est automatiquement privilégié, sans que la personne n'ait à faire quoi que ce soit d'autre. Or, cette méthode peut fonctionner pour toutes sortes de services, mais peut-être pas dans tous les cas.

Aux termes de notre loi actuelle, si elle est bien mise en oeuvre, le deuxième principe dit qu'il faut déterminer les fins du traitement, de la collecte, de l'utilisation et de la divulgation des renseignements personnels.

Selon le principe suivant, il faut obtenir le consentement, et nous savons maintenant que celui-ci doit être valable. Il y a une certaine marge de manoeuvre du fait que la forme du consentement doit être choisie en fonction de la sensibilité des renseignements. Or, cela ne signifie pas nécessairement que le consentement actif s'applique uniquement aux aspects les plus sensibles. Il y a toute une gamme de situations. Des éléments propres à l'utilisation d'un service en font partie intégrante, en quelque sorte. Faut-il une case à cocher pour donner son consentement? Si je commande un livre chez Chapters-Indigo, dois-je donner mon consentement actif pour autoriser l'entreprise à utiliser l'adresse que je viens de lui fournir afin de m'envoyer le livre? La réponse est tout à fait évidente dans cette transaction, et ce consentement devrait être implicite. En revanche, une utilisation secondaire comme l'emploi de mon nom et de mon adresse aux fins de marketing, entre autres, semble être un élément sensible qui nécessite un consentement actif.

L'un des grands avantages de la loi, c'est qu'elle repose sur des principes et qu'elle laisse une certaine latitude, de sorte qu'elle fonctionne dans les modèles tant de Chapters et d'une banque que des télécommunications.

● (1715)

M. Nathaniel Erskine-Smith: J'ai une dernière question. Vous avez mentionné l'importance du choix, ce pour quoi il ne faut pas délaisser le modèle de consentement. Tandis que les conditions d'utilisation sont de plus en plus complexes, et que nous adhérons à de nombreux services différents, je remarque que l'Ontario a déjà un modèle depuis des dizaines d'années. La Loi sur la vente d'objets parle de garanties implicites et prévoit des modalités de base auxquelles les consommateurs ne peuvent pas renoncer. Ainsi, les entreprises ne peuvent pas permettre aux consommateurs d'y renoncer pour leur propre protection. Pensez-vous que les mêmes principes pourraient s'appliquer à la protection de la vie privée?

M. David Fraser: Je doute que l'analogie soit parfaite, et j'hésiterais à concrétiser quoi que ce soit étant donné que la technologie et les attentes des consommateurs vont évoluer. Mais je pense qu'il est logique d'inscrire des indications comme « si ce sont vos pratiques par défaut », « voici vos conditions d'utilisation générales », ou encore « vous avez ici une politique normale sur la protection des renseignements personnels ». Ainsi, on s'attend à ce qu'il n'y ait rien d'autre à faire pour obtenir un consentement additionnel. Mais si on déroge de cette voie, il serait peut-être bien de le faire savoir à la personne. En ce qui concerne les lacunes relevées, je doute que bien des entreprises respectent pleinement leurs obligations en vertu de la LPRPDE, en ce qui concerne la détermination des fins. Tout le monde pourrait faire un meilleur travail à ce chapitre. Il est question des avis abrégés sur la protection des renseignements personnels, comme l'étiquetage nutritionnel et les avis juste à temps. J'avertis mes clients que personne ne lira leur politique sur la protection des renseignements personnels. Ils ne peuvent pas compter là-dessus pour la détermination des fins et le consentement. Lorsqu'ils demandent des renseignements à leurs consommateurs au moyen d'un formulaire, ils doivent leur indiquer clairement ce qu'ils vont en faire. Dans le cas contraire, les politiques sur la protection des renseignements personnels ne sont pas plus qu'une fiction juridique.

Le président: Très bien. Chers collègues, la sonnerie ne s'est pas encore fait entendre, mais je vois à l'écran que le Président est en train de lire la motion, de sorte que les cloches commenceront à retentir sous peu. Nous allons donc émettre cette hypothèse.

Je voudrais tout d'abord m'excuser auprès de nos témoins. Ce genre de chose se produit de temps à autre, mais je vous remercie infiniment de votre écoute et de votre patience pendant nos délibérations d'aujourd'hui.

S'il y a autre chose que nous devrions savoir, ou d'autres réponses que vous auriez voulu nous donner, nous vous prions de faire parvenir ces renseignements au Comité. Nous vous invitons aussi à suivre la suite de notre étude sur la LPRPDE. Si vous pensez à quoi que ce soit d'autre qui pourrait être dans l'intérêt de tous les Canadiens, faites-le-nous savoir.

Merci beaucoup.

La séance est levée.