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 044 • 1re SESSION • 41e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 7 juin 2012

Président

M. Pierre-Luc Dusseault

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

Le jeudi 7 juin 2012

● (1135)

[*Français*]

Le président (M. Pierre-Luc Dusseault (Sherbrooke, NPD)): Nous allons maintenant entamer la séance.

Je tiens à remercier les témoins que nous allons entendre aujourd'hui par l'entremise d'une vidéoconférence. Il va y avoir une présentation de 10 minutes de la commissaire à l'information et à la protection de la vie privée de l'Ontario et une autre de 10 minutes, également, de la commissaire à l'information et à la protection de la vie privée de la Colombie- Britannique.

Comme nous disposons de beaucoup moins de temps aujourd'hui, je vais sans plus tarder céder la parole à Mme Denham.

[*Traduction*]

Mme Elizabeth Denham (commissaire, Bureau du Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique): Monsieur le président, mesdames et messieurs les membres du comité, merci beaucoup de nous avoir invitées aujourd'hui.

Je suis venue en compagnie de Caitlin Lemiski et d'Helen Morrison, qui sont toutes deux analystes principales des politiques dans mon service.

J'ai comparu pour la première fois devant le comité alors que j'étais commissaire adjointe à la protection de la vie privée du Canada et en février dernier je suis à nouveau venue témoigner devant vous à titre de registraire des lobbyistes de la Colombie-Britannique.

Lorsque j'étais commissaire adjointe à la protection de la vie privée du Canada, j'ai dirigé la première enquête jamais consacrée à une plate-forme de médias sociaux par une autorité de protection des données. En qualité de commissaire à l'information et à la vie privée de la Colombie-Britannique, j'ai mené la toute première enquête au Canada sur l'utilisation d'un site de médias sociaux par un parti politique. À la suite de cette enquête, nous avons publié des lignes directrices sur la vérification des antécédents sur les sites de médias sociaux.

Aujourd'hui, j'aimerais vous offrir un aperçu du modèle de surveillance de la Colombie-Britannique. Je passerai ensuite en revue quelques-uns de nos travaux récents dans le domaine des médias sociaux, puis j'exposerai mon point de vue sur l'adéquation entre les lois canadiennes sur la protection de la vie privée et les défis liés aux médias sociaux ainsi que sur la façon dont les gouvernements pourraient renforcer l'application de nos lois.

Pour réglementer le secteur privé, le Commissariat à l'information et à la vie privée surveille et applique la Loi sur la protection des renseignements personnels de la Colombie-Britannique, la PIPA. La PIPA détermine quels renseignements personnels les organisations peuvent recueillir, utiliser ou divulguer. Nous partageons l'espace de réglementation avec le commissariat fédéral, parce que la PIPA de la Colombie-Britannique a été déclarée essentiellement similaire à la LPRPDE. La PIPA a toutefois une vaste portée. Elle s'applique aussi aux organisations sans but lucratif et englobe les renseignements personnels des employés.

La PIPA donne au commissaire le pouvoir de rendre des ordonnances. Je peux par exemple ordonner à une organisation de cesser de recueillir, d'utiliser ou de divulguer des renseignements personnels. Je peux aussi exiger d'une organisation qu'elle supprime des renseignements personnels recueillis en contravention de la loi. D'après mon expérience, le pouvoir de prendre des ordonnances me dote de l'autorité nécessaire pour veiller à ce que les entreprises respectent les obligations qui découlent de la loi.

La PIPA régit les pratiques des entreprises et des organisations dans le domaine des renseignements personnels de façon à reconnaître aussi bien le droit à la vie privée des particuliers que le besoin des organisations de recueillir des renseignements personnels à des fins raisonnables. Compte tenu de cette approche équilibrée, les lois sur la protection de la vie privée n'empêchent ni ne devraient empêcher les organisations de mettre au point et d'utiliser des technologies avantageuses pour l'économie numérique.

Je suis parfaitement consciente du caractère innovateur et du grand intérêt des médias sociaux. Ils permettent aux utilisateurs de s'exprimer de façon nouvelle et stimulante et ils favorisent la participation du public. Les médias sociaux aident aussi les utilisateurs à rester en contact avec leurs parents et leurs amis, à se tenir au courant de l'information et à constituer des communautés virtuelles.

Cela dit, je partage les préoccupations de la commissaire à la vie privée du Canada au sujet des entreprises de médias sociaux qui ne respectent peut-être pas suffisamment les lois canadiennes en matière de protection de la vie privée. Toutes les organisations, y compris les entreprises de médias sociaux, doivent respecter les règles relatives à la connaissance et au consentement ainsi que les limites imposées à la collecte, à l'utilisation et à la conservation de renseignements personnels. Ces règles sont d'autant plus importantes que l'information peut être diffusée et reproduite très rapidement dans les médias sociaux.

Je suis également consciente du fait que ces entreprises fonctionnent dans un contexte international, ce qui est susceptible de compliquer les choses. En matière de protection de la vie privée, le Canada a un cadre législatif très différent de celui des États-Unis, où la majorité des sites les plus populaires au monde sont basés. Toutefois, cela n'exempte pas les entreprises de médias sociaux de respecter les lois canadiennes sur la protection de la vie privée. Toutes les organisations qui travaillent sur notre territoire doivent rendre compte de leurs pratiques de gestion des renseignements personnels. Elles doivent respecter la loi.

Certaines enquêtes récentes menées par les commissariats canadiens montrent que le Canada est en mesure de calmer certaines préoccupations relatives aux médias sociaux et à la vie privée. Toutefois, c'est un combat qui est constamment à recommencer.

● (1140)

En Colombie-Britannique, nous avons récemment enquêté sur la collecte de mots de passe et de profils Facebook par un parti politique qui utilisait cette information pour vérifier les antécédents d'éventuels candidats au leadership. Nous avons constaté que même si le parti politique sollicitait le consentement des candidats, la collecte des mots de passe et de l'information contenue dans les profils contrevenait à la loi. La PIPA stipule qu'une organisation peut recueillir de renseignements personnels uniquement à des fins qu'une personne raisonnable considérerait appropriées.

Nous avons également découvert que lorsqu'ils prenaient connaissance des profils que les candidats publiaient dans les médias sociaux, les représentants du parti politique recueillaient aussi de l'information sur les amis et les amis des amis des candidats, sans les en informer ni leur demander leur consentement. À la suite de notre enquête, le parti a accepté de mettre un terme à la collecte de mots de passe et d'adopter les lignes directrices publiées par notre service au sujet des vérifications des antécédents dans les médias sociaux.

Dans le cadre d'une autre enquête, nous nous sommes penchés sur le cas de l'Insurance Corporation de la Colombie-Britannique, qui avait offert au service de police de Vancouver d'utiliser sa base de données de reconnaissance faciale afin d'identifier des personnes qui auraient pu participer aux émeutes de la Coupe Stanley en 2011. Le lien entre les entreprises de médias sociaux et la technologie de reconnaissance faciale est très important, car nombre de ces entreprises intègrent cette technologie dans leurs applications. L'an dernier, par exemple, Facebook a intégré la reconnaissance faciale à ses services photographiques, pour permettre le repérage automatique de personnes dans les photos téléchargées. Facebook a décidé de ne pas activer cette fonction au Canada.

De fait, l'offre de l'ICBC au service de police de Vancouver nous a fait prendre plus pleinement conscience du pouvoir de la technologie de reconnaissance faciale et de son intérêt pour les services policiers. L'utilisation des médias sociaux par les policiers suscite une préoccupation particulière, car les collections de photographies de personnes des entreprises de médias sociaux sont parmi les plus importantes au monde.

On peut se demander si les personnes autorisent en toute connaissance de cause la collecte de renseignements biométriques pour la reconnaissance faciale. Si cette information est recueillie sans autorisation préalable, son utilisation subséquente par les policiers pourrait être illégale. En outre, des tests ont remis en question la fiabilité de cette technologie. Dans un aéroport américain, par exemple, un projet pilote de reconnaissance faciale a permis d'identifier correctement seulement 61 p. 100 des volontaires qui participaient à l'expérience. En raison de ce faible taux de succès, l'aéroport a abandonné son projet d'utiliser la reconnaissance faciale. Ces questions continuent toutefois de se poser, car la technologie s'améliore et qu'un jour ou l'autre les policiers voudront l'utiliser. Le rapport entre les policiers et les médias sociaux, particulièrement dans le cas des logiciels de reconnaissance faciale, est un aspect qui mériterait plus d'attention et devrait être étudié plus à fond.

Les exigences de la loi, quelles qu'elles soient, sont sans grand effet si les organisations ne les respectent pas. Selon moi, le principal défi pour la protection de la vie privée dans le contexte des médias sociaux vient du fait que les entreprises connaissent mal l'obligation de limiter le type de renseignements personnels qu'elles recueillent. Par exemple, en Colombie-Britannique, de nombreuses organisations ignorent que la PIPA leur interdit de recueillir des renseignements personnels pour la simple raison que ces renseignements sont disponibles sur le Web et elles sont étonnées de l'apprendre.

Dans le contexte des vérifications préalables à l'emploi, l'approche désinvolte d'une organisation en matière de collecte de renseignements personnels en ligne peut avoir des résultats pour le moins troublants. Par exemple, il serait normalement inapproprié et illégal pour un employeur de recueillir des renseignements concernant l'âge ou l'orientation sexuelle d'un candidat à l'emploi ou encore le fait qu'il ait ou non des enfants, mais l'employeur peut prendre connaissance de ces détails en consultant le profil du candidat dans les médias sociaux. Les renseignements personnels affichés sur ces sites sont souvent inexacts. En outre, un peu comme les pêcheurs qui pêchent au filet, les organisations peuvent recueillir beaucoup plus de renseignements personnels que ce qu'elles cherchent lorsqu'elles relèvent de l'information sur ces sites Web.

Certains considèrent que les utilisateurs doivent assumer la responsabilité de ce qu'ils diffusent en ligne. Il est vrai qu'il faut réfléchir avant d'afficher des renseignements, mais cela ne signifie pas que nous devrions restreindre les occasions raisonnables de nous exprimer. Finalement, c'est une question de contexte et, au Canada, les lois sur la protection de la vie privée reconnaissent cette réalité en limitant la collecte et l'utilisation des renseignements en fonction de ce qui est raisonnable dans les circonstances.

À mesure que les opinions des Canadiens en matière de communication et d'expression évoluent, le défi pour les commissariats et les gouvernements consistera à aider les organisations à comprendre ces nouvelles distinctions. Une mère ne devrait pas s'interdire d'afficher des renseignements sur son expérience parentale par crainte de répercussions de la part de son employeur, et des amis devraient pouvoir commenter librement des produits et services sans être indûment surveillés et profilés par le marché.

Ces observations confirment ce qu'on peut lire dans un rapport publié en 2010 par le Commissariat à la protection de la vie privée du Canada: « les concepts traditionnels d'espaces publics et privés sont en train de changer. Les Canadiens continuent de considérer la protection de la vie privée comme importante, mais ils veulent également participer à la vie en ligne. » Il faudra déployer des efforts soutenus d'éducation publique et de mobilisation pour encourager le respect des lois canadiennes sur la vie privée dans l'univers des médias sociaux.

Pour conclure, les entreprises de médias sociaux devraient utiliser les innovations qui les rendent si populaires pour protéger la vie privée dont les Canadiens sont jaloux. La protection de la vie privée ne se limite pas à l'obtention d'un consentement éclairé. Il faut aussi faire ce qu'il convient de faire en fonction des circonstances.

Les lois axées sur les principes et neutres sur le plan technologique s'adaptent aux nouvelles technologies, mais je crois qu'il est essentiel que le commissariat fédéral dispose d'outils d'application puissants, notamment le pouvoir de rendre des ordonnances et le signalement obligatoire des violations, pour pouvoir réglementer cet espace.

Je vous remercie infiniment de m'avoir offert cette occasion de témoigner aujourd'hui et je répondrai avec plaisir à vos questions.

● (1145)

[*Français*]

Le président: Merci.

Sans plus tarder, je vais donner la parole à Mme Cavoukian, avec qui nous serons en contact à partir de Toronto et dont l'intervention sera de 10 minutes.

[*Traduction*]

Mme Ann Cavoukian (commissaire, Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario): Mesdames et messieurs, bonjour. Je remercie le président et les membres du comité de m'avoir invitée à prendre la parole aujourd'hui.

Je ne vais pas vous parler de la réglementation et des lois existantes en matière de protection de la vie privée. La commissaire Stoddart l'a déjà fait devant votre comité. Vous avez entendu le témoignage de juristes comme Michael Geist. Vous venez d'entendre Mme Denham. Il faut faire un travail très important dans la sphère réglementaire et législative.

Si je ne vous parle pas de ces questions aujourd'hui, ce n'est pas faute de disposer d'une réglementation solide dans ma province; j'ai le pouvoir de rendre des ordonnances et je ne saurais trop insister sur l'importance de ce pouvoir pour un organisme de réglementation. J'ai aussi, en vertu de la LPRPS, une merveilleuse capacité en ce qui concerne le signalement obligatoire des violations. Nous possédons ces outils, ils sont excellents, mais je ne vais pas vous en parler aujourd'hui.

Je vais vous parler de l'avenir de la protection de la vie privée. J'ai 10 minutes pour vous parler de ce que l'on appelle la protection intégrée de la vie privée. Auparavant, toutefois, permettez-moi de présenter mes collègues. Je suis venue en compagnie de Michelle Chibba, directrice des politiques, et de David Goodis, directeur des services juridiques.

La protection intégrée de la vie privée vise à garantir que l'utilisateur détermine ce qui est fait de ses renseignements personnels. Vu la croissance effrénée des technologies mobiles, l'omniprésence du sans-fil, la popularité des médias sociaux en ligne et des dispositifs portables, toutes les possibilités de partage de l'information et la disponibilité de l'information, il devient de plus en plus difficile, dans le monde, de réglementer strictement l'information a posteriori — une atteinte à la vie privée se produit, une plainte est déposée, nous faisons enquête et nous offrons un recours. Cette façon de procéder est utile et doit être maintenue, mais avec ces outils nous ne voyons, selon moi, que la pointe de l'iceberg en ce qui concerne les violations de la vie privée et les activités qui empiètent sur la vie privée. La protection intégrée de la vie privée permet d'être proactif et d'essayer de prévenir les atteintes à la vie privée.

Vous savez qu'il y a deux ans, à Jérusalem, la communauté internationale des commissaires à la protection de la vie privée et des responsables de la protection des données ont consacré la protection intégrée comme norme internationale. Cette décision a été prise à l'unanimité et, depuis, cette norme est reflétée dans des travaux présentés par les États-Unis et l'UE. Aux États-Unis, la FTC, la commission fédérale du commerce, a publié en janvier dernier sa vision de l'avenir de la protection de la vie privée en termes de structure réglementaire et d'autoréglementation du secteur privé. Elle recommande trois pratiques, et en premier lieu d'adopter le concept de la protection intégrée de la vie privée.

Si vous regardez la réglementation que l'UE a présentée cette année en matière de protection des données, vous y trouverez la protection intégrée, et le principe de la protection de la vie privée comme option implicite imprègne toute la réglementation. Je vous signale que la protection intégrée est maintenant traduite en 25 langues. Je vous assure que c'est un exploit. Elle est exprimée dans toutes les grandes langues du monde. Cela vous donne une petite idée de l'importance du principe de protection intégrée et de l'intérêt qu'il suscite dans le monde.

Je vais maintenant traiter rapidement des sept principes fondateurs de la protection intégrée. Je vous les résume. Le concept prévoit, essentiellement, l'intégration de fonctions de protection de la vie privée non seulement dans les technologies de l'information mais aussi dans les pratiques, politiques et procédures commerciales responsables, de façon proactive, pour prévenir les atteintes à la vie privée plutôt que d'y réagir après coup.

● (1150)

La caractéristique fondamentale de la protection intégrée est d'être le réglage implicite. La protection de la vie privée est donc la condition de base, et vous, les utilisateurs, les personnes visées par les renseignements, savez que vos renseignements sont protégés. Vous n'avez pas à prendre de mesure particulière. Cela est garanti. Cela est automatique. Cela est intégré dans le système: c'est le réglage implicite. C'est la clé, et c'est un aspect fondamental de la protection intégrée.

L'autre caractéristique essentielle est un contexte à somme positive plutôt que nulle. Dans un contexte à somme nulle, vous ne pouvez avoir que l'un ou l'autre de deux intérêts: vous pouvez avoir la protection de la vie privée ou la sécurité, la protection de la vie privée ou les médias sociaux, la protection de la vie privée ou les fonctions biométriques. Dans tous ces binômes, vous pouvez maintenant enlever le « ou ».

Dans un contexte à somme positive, la protection de la vie privée s'harmonise à d'autres fonctions. Il faut que la vie privée soit protégée dans un cadre où elle peut fonctionner à l'unisson avec d'autres intérêts, cela est essentiel. L'avenir sera marqué par la créativité et l'innovation. Qui sait ce qui s'annonce en matière de technologie et de progrès? Cela est positif. Nous insistons pour que la protection de la vie privée figure dans cet ensemble.

Nous avons tous beaucoup entendu parler des mégadonnées. Je n'aborderai pas cette question avec vous aujourd'hui, je n'ai pas assez de temps. Toutefois, pour éveiller votre curiosité, je vous annonce que nous publions demain un document réalisé conjointement avec IBM et intitulé *Privacy by Design in the Age of Big Data*. Nous le rendons public demain matin, à l'occasion de conférences qui auront lieu à Washington et à Toronto. Si vous visitez notre site Web demain, jetez-y un oeil pour savoir comment nous pouvons à la fois protéger la vie privée et profiter des mégadonnées.

Il me reste quatre minutes pour vous présenter un exemple concret de protection intégrée. Je ne veux pas que vous pensiez qu'il s'agit d'un concept théorique ou d'une invention d'universitaire. Cela est concret. Cela fonctionne déjà.

Je tire mon exemple de Facebook et d'autres médias sociaux. Comme Mme Denham le mentionnait, Facebook a instauré une fonction de reconnaissance faciale. Les photos téléchargées dans Facebook peuvent être marquées au moyen de la technologie de reconnaissance faciale. Vous imaginez bien la mine d'information que représentent toutes ces images pour les services policiers et pour d'autres intérêts. Les visages de quelque 900 millions d'utilisateurs seraient marqués au moyen la technologie de reconnaissance faciale et pourraient être comparés à des photos prises sur la scène d'un crime, par exemple. Les policiers se présenteraient aux bureaux de Facebook munis d'un mandate, évidemment, Facebook n'aurait d'autre choix que de leur remettre l'information.

Je vais vous parler d'une technologie que nous avons adoptée ici, en Ontario, pour que cela soit impossible, même si la technologie de reconnaissance faciale se perfectionne. Il s'agit de la technologie de reconnaissance faciale avec chiffrement biométrique intégré pour protéger la vie privée.

Je vous explique rapidement de quoi il s'agit. En Ontario, la Société des loteries et des jeux de l'Ontario, OLG, gère les casinos de la province. Nous avons 27 casinos et ils sont tous gérés par OLG.

La société m'a consultée, il y a quelques années. Elle avait un programme pour les joueurs compulsifs appelé Programme d'auto-exclusion. Si vous avez un problème de jeu, vous pouvez suivre un programme en 12 étapes, Gamblers Anonymous par exemple, et à la fin du programme vous devez aller dans un casino pour vous inscrire au programme d'auto-exclusion. Vous voulez renoncer au jeu. Vous avez suivi le programme au complet, mais vous savez que vous pourriez faire une rechute et retourner jouer dans un casino. Vous ne voulez pas que cela se produise.

Le programme d'auto-exclusion est entièrement volontaire. Il suffit d'aller au casino et de dire « Inscrivez-moi. Je veux que vous m'empêchiez d'entrer. Si vous me voyez entrer, j'aimerais que vous me demandiez de partir, s'il vous plaît. » Vous remplissez le formulaire, vous vous faites photographier et vous signez. C'est votre décision, ce que vous voulez faire.

Malheureusement, le programme ne donnait pas toujours les résultats escomptés. Par le passé, le formulaire et la photo étaient rangés dans un bureau quelque part, dans un classeur.

● (1155)

Les joueurs compulsifs qui rechutaient essayaient de retourner au casino. Ils rentraient par la grande porte — il y a 27 casinos dans la province — et ils n'avaient aucune difficulté. Ils étaient très habiles et ils réussissaient à entrer. Un grand nombre de ces malheureux ont ainsi perdu toutes leurs économies. Ils ont perdu leur famille. Ils ont perdu leur emploi. Ce sont de terribles conséquences. Ensuite, ils poursuivaient le gouvernement ontarien — le casino —, qui n'avait pas respecté le programme pour les exclure. Tous y perdaient.

Lorsque les représentants d'OLG sont venus nous voir et nous ont demandé une solution, ils nous ont proposé ce qui suit. Il y a des caméras à l'entrée de tous les casinos. Les casinos du monde entier ont des caméras à l'entrée, à des fins de sécurité. Les représentants d'OLG ont expliqué que s'ils comparaient les images prises par ces caméras avec les photographies stockées dans des fichiers à l'arrière du casino, ils pourraient repérer les joueurs qui avaient signé un formulaire d'auto-exclusion et les empêcher d'entrer.

Par contre, cela crée un problème. La technologie de reconnaissance faciale photographie les visages de toutes les personnes qui entrent dans le casino, pas seulement ceux des joueurs compulsifs, et cette information pourrait ensuite être remise à des utilisateurs secondaires, notamment les services de police. Je voulais empêcher que cela se produise.

Nous leur avons donc demandé d'utiliser un programme de chiffrement biométrique. En gros, c'est un système qui permet d'utiliser les données de reconnaissance faciale de telle sorte qu'elles ne peuvent servir à aucune autre fin. Quand vous utilisez le chiffrement biométrique, aucun gabarit biométrique — comme on appelle la représentation numérique du visage ou de l'empreinte digitale — n'est conservé dans la base de données.

C'est donc dire que si les policiers viennent vous demander l'accès à votre base de données de gabarits biométriques pour essayer d'y trouver la photo d'un suspect, c'est impossible parce qu'il n'existe aucune image. L'information peut être utilisée uniquement à cette fin précise, uniquement dans le but visé.

Si nous avons le temps, je vous expliquerai ultérieurement le comment fonctionne ce système. Disons toutefois que cette technologie a été testée ailleurs dans le monde. Aux Pays-Bas, priv-ID, une autre entreprise, l'a fait, et je peux vous donner d'autres exemples.

C'est une solution biométrique avec protection intégrée qui est merveilleuse et qui permet d'utiliser la technologie biométrique sans que les renseignements puissent servir à d'autres fins que les fins visées.

● (1200)

[*Français*]

Le président: Pardonnez-moi, mais je dois vous aviser qu'il vous reste environ une minute pour conclure votre présentation.

[*Traduction*]

Mme Ann Cavoukian: Je vous demande d'envisager d'adopter la protection intégrée comme solution permanente pour la protection de la vie privée. Si nous demandons par exemple à Google, à Facebook et à d'autres entreprises d'adopter des solutions de protection intégrée comme le chiffrement biométrique dans leurs programmes de reconnaissance faciale, notre vie privée sera beaucoup mieux protégée et nous pourrons continuer à nous prévaloir des fonctions offertes par les médias sociaux grâce à ce programme particulier.

Vous pouvez assurer à la fois la protection de la vie privée et d'autres fonctions de base, mais je vous prie instamment de n'en autoriser aucune aux dépens de la protection de la vie privée.

Merci beaucoup, mesdames et messieurs.

[*Français*]

Le président: Merci.

Je vais maintenant céder la parole à M. Angus, qui dispose de sept minutes.

[*Traduction*]

M. Charlie Angus (Timmins—Baie James, NPD): Merci beaucoup.

D'entrée de jeu, madame Denham et madame Cavoukian, je dois vous féliciter du leadership que vous manifestez dans le dossier des droits des Canadiens en matière de vie privée. Vous êtes toutes les deux des championnes à cet égard et vous faites preuve d'une grande prévoyance. Vos efforts ont été très utiles.

Je m'intéresse à la question de la protection intégrée parce que lorsque nous légiférons les solutions nous arrivons toujours après le fait, nous accusons toujours du retard et nous encourageons pas la création du genre d'univers de médias sociaux que nous voudrions avoir.

Le concept de protection intégrée me fascine, et j'espère que notre comité l'étudiera sérieusement. Je compare cela aux enjeux de l'industrie forestière dans les années 1990 au Canada et aux combats des groupes environnementaux. À cet époque, les conflits semblaient devoir perdurer indéfiniment, jusqu'à ce que les parties commencent à collaborer pour établir une norme, la certification en foresterie, la certification du FSC. Il y a encore bien des problèmes liés à cette certification, mais elle est devenue une norme qu'il faut respecter pour réussir à aller au-delà des conflits perpétuels dans le secteur forestier.

Il me semble que cela nous aiderait à progresser dans le dossier de la vie privée. Je me demande s'il faut légiférer son adoption? Devons-nous simplement espérer que les géants et les petits joueurs vont l'adopter? Est-ce qu'il y a une façon de dire qu'au Canada, il faut instaurer ce système, que c'est la règle absolue et que nous exigeons son respect? Comment pouvons-nous parvenir à cela, concrètement?

Mme Ann Cavoukian: Merci beaucoup de cette question.

Je crois qu'il y a une façon d'y parvenir. Je vous renvoie à un document que nous avons publié l'été dernier — attendez que je me souvienne du titre... *Privacy by Design in Law, Policy and Practice*. L'idée est venue de la commissaire Pamela Jones Harbour, qui était autrefois membre de la FTC. Lorsqu'elle m'a parlé de la protection intégrée, elle m'a dit que nous pouvions l'imposer comme exigence, en faire une condition, dans les décrets de consentement, dans les décisions que publie la FTC à la fin d'une enquête, et que nous pourrions l'inclure en permanence pour que les entreprises soient tenues de l'appliquer de façon proactive par la suite.

Le juge La Forest a eu la bonté d'examiner le document que je viens de mentionner et qui se trouve sur notre site Web. Il considère que la protection intégrée est une excellente idée qui devrait être ajoutée aux moyens administratifs prévus dans la loi pour régler de façon continue les questions soulevées par la protection de la vie privée.

Nous pourrions le faire, entre autres — et je sais que le projet de loi C-12 envisage des changements de la LPRPDE — serait de décréter qu'après une enquête, l'entreprise est tenue d'appliquer en permanence le principe de la protection intégrée dans tout secteur où des problèmes sont repérés.

La protection intégrée de la vie privée, ce n'est pas une punition. Nous disons toujours que la protection est excellente pour les affaires. Elle devrait assurer certains avantages aux entreprises qui ont de bonnes pratiques en la matière. La confiance des consommateurs s'érode très rapidement de nos jours, et il est bon de la renforcer chez vos clients. Ce n'est pas vraiment un bâton. C'est à la fois une carotte et une mesure d'encouragement pour faire adopter des mesures de protection de façon à économiser des ressources, parce que l'entreprise pourra ainsi éviter les violations, les enquêtes et, le cas échéant, les recours collectifs.

Il se passe tant de choses en matière de protection de la vie privée que lorsque nous discutons de la protection intégrée de la vie privée avec des entreprises, c'est parce qu'elles nous ont invités à le faire. Elles sont disposées à adopter ce concept non seulement pour les bonnes raisons, mais aussi parce qu'elles y voient des avantages commerciaux.

Je crois qu'une solution consisterait à intégrer ce principe dans de nouvelles structures de réglementation.

● (1205)

M. Charlie Angus: Merci. Je crois que c'est une façon intéressante d'envisager la question.

Je ne pense pas que les entreprises du secteur des médias sociaux cherchent délibérément à recueillir des données pour les diffuser. Ce sont plutôt des conséquences fortuites, et cela crée un véritable paradis pour les prédateurs.

Mme Ann Cavoukian: Oui.

M. Charlie Angus: Les jeunes publient toutes sortes d'images dans Facebook, et tout est marqué. Si quelqu'un décide de harceler ou de suivre une personne ou de lui empoisonner la vie, la technologie est très simple, il y a des conséquences fortuites que personne n'a nécessairement anticipées au départ. Si nous intégrons ce principe dans le système d'exploitation, les gens n'auront pas à se soucier de ces possibilités.

Est-ce que nous devons attendre que quelques gros joueurs s'engagent sur cette voie de façon proactive? Vous disiez qu'il y avait beaucoup de soutien au plan international. Comment pouvons-nous vraiment mettre cela en oeuvre?

Mme Ann Cavoukian: Monsieur Angus, je suis heureuse que vous parliez de conséquences fortuites. Je ne l'ai pas projetée ici, mais j'ai une diapositive que j'utilise plus particulièrement quand je m'adresse à des entreprises de technologie. Elle porte simplement ces mots: Attention aux conséquences fortuites. C'est toujours un danger.

J'ai dit que l'année dernière avait été l'année de l'ingénieur, parce que j'ai parlé à des ingénieurs dans toutes les grandes sociétés du monde. J'ai discuté avec Adobe. J'ai discuté avec Intel et HP, avec Google... J'ai rencontré Facebook et d'autres aussi, mais je voulais surtout parler à leurs ingénieurs, à leurs équipes d'informatique, pour traduire ou opérationnaliser dans des codes, en quelque sorte, les principes de la protection intégrée.

Évidemment, nous discutons depuis des années avec les avocats, je ne suis pas inquiète pour les avocats et les rédacteurs de politiques. Ils savent comment traduire en codes les exigences de la politique, etc. Par contre, les ingénieurs n'étaient pas inclus, et les informaticiens non plus. Je leur ai dit que c'était fort simple, que je ne pouvais pas rédiger le code à leur place mais que je pouvais leur expliquer ce qu'était un but premier et comment il fallait faire en sorte que les procédures opérationnelles de l'entreprise reflètent les principes de minimalisation des données.

La protection implicite est une fonction essentielle. Nous essayons d'expliquer cela non seulement aux ingénieurs — et ils le comprennent, bien sûr — mais aussi aux non-initiés. J'utilise toujours ce que j'appelle mon test des voisins. J'ai des voisins très intelligents, très futés, qui ne travaillent pas dans le domaine de la protection de la vie privée. Alors j'essaie d'expliquer les choses à mes voisins, et s'ils comprennent le concept, et ils le comprendront, c'est qu'il est au point. Il faut qu'il soit accessible tant au public qu'aux ingénieurs, et la notion de protection de la vie privée comme réglage implicite est un concept efficace. Une de mes voisines m'a répondu, est-ce que cela signifie que c'est gratuit? Je n'ai pas besoin de le demander? Je n'ai pas à consulter la politique pour le découvrir? Je l'ai gratuitement? J'ai répondu que oui, que c'était implicite dans le système, que c'était une fonction automatique. C'est parfait, m'a-t-elle dit, c'est cela que je veux.

Nous avons ce genre de discussions. Comme je l'ai dit, nous nous sommes adressés à toutes les grandes entreprises. Dans le cas de Google+, nous avons participé avec l'entreprise aux essais beta de Google+, le nouveau média social. Les responsables s'intéressaient de près aux questions de protection de la vie privée. Ils ont produit ce concept des cercles qui permettent limiter les renseignements personnels et ce qu'on partage au moyen de cercles. Vous pouvez avoir un cercle pour vos collègues, un autre pour vos voisins, un pour la famille, etc.

Nous avons discuté de la protection intégrée avec toutes les grandes sociétés. Je crois que si vous vous adressiez à l'une ou l'autre d'entre elles, vous constateriez qu'elles sont au courant du concept.

● (1210)

[*Français*]

Le président: Merci.

Malheureusement, votre temps de parole est écoulé, monsieur Angus. Comme vous le savez, la période de sept minutes inclut les questions et les réponses.

Je cède maintenant la parole à M. Calkins, qui dispose de sept minutes.

[*Traduction*]

M. Blaine Calkins (Wetaskiwin, PCC): Merci, monsieur le président. Je remercie nos témoins d'aujourd'hui.

Il est agréable d'accueillir deux commissaires provinciales. Vos exposés reflètent certainement une grande expérience.

J'aborde la question du point de vue du programmeur qui s'est souvent heurté à certaines de ces questions dans une vie antérieure, avant de devenir député.

M. Michael Geist a comparu devant le comité il y a quelques jours — et je crois que c'était un peu le sens des questions de M. Angus... Je m'inquiète énormément, non seulement comme consommateur et comme utilisateur de l'Internet, ces jours-ci, mais aussi parce que j'ai de jeunes enfants et que la situation m'inspire des craintes. Évidemment, à titre de député je m'inquiète toujours des questions de protection de la vie privée de mes électeurs. L'étude que nous réalisons actuellement est donc opportune et intéressante.

Je suis parfaitement d'accord pour ce qui est de la protection implicite... M. Geist disait que le diable se cache dans les réglages implicites. Il me semble que nous devrions nous inquiéter de certains des réglages implicites qui sont utilisés, que ce soit au niveau du système d'exploitation, au niveau du fureteur ou de l'interface ou encore au niveau des données. J'aimerais donner à nos deux témoins l'occasion de parler un peu de cela.

Je suis certainement d'accord avec vous — et dans votre exposé sur la protection intégrée, c'est le deuxième principe, la protection implicite —, c'est un élément qui, selon moi, plairait bien à la majorité des Canadiens si on le leur expliquait clairement.

Je voudrais aussi que l'on me demande explicitement à moi, le consommateur, l'autorisation de recueillir des renseignements personnels. Cela ne devrait pas être mentionné seulement dans un document juridique de 15 pages, un document que je dois accepter en bloc en appuyant sur un petit bouton. Il m'est impossible d'accepter certains éléments de ce document et de rejeter les autres, je dois tout accepter et signer pour ouvrir un compte, par exemple, ou pour conclure une transaction.

Je me demande si vous pouvez nous suggérer des pratiques ou des recommandations pour aider les consommateurs à s'y retrouver sur cette toile de plus en plus complexe.

Mme Elizabeth Denham: Je considère que le consentement est très important dans le cyberespace, mais c'est seulement un élément de réponse. Je suis d'accord avec vous, ce ne sont pas les ententes avec les utilisateurs finaux, avec leurs longs préavis et leurs jargon juridique, qui vont régler le problème. Un excellent travail a été réalisé en matière de courts préavis, de préavis juste à temps. C'est encore plus important dans le cas des appareils portables, parce qu'on ne peut pas lire le consentement ou la convention d'utilisateur.

Les lois canadiennes sont souples. Elles exigent que la collecte de données soit raisonnable et elles créent une obligation de transparence. Dans un écosystème complexe comme un site de média social, cela est difficile parce qu'à mon avis, le consommateur comprend mal ce qui se cache derrière l'écran. Il n'est pas conscient de tous les groupes avec qui il communique, il ignore comment les données circulent et comment des tierces parties peuvent utiliser ses renseignements. C'est un univers entièrement nouveau.

Autrefois, le consommateur traitait avec une entreprise qui avait pignon sur rue. Il savait très bien à qui il avait affaire. Le consentement était suffisant dans ce contexte. Je crois qu'aujourd'hui, il nous faut une approche beaucoup plus perfectionnée.

Il faut commencer par la responsabilisation. Notre bureau, en collaboration avec l'Alberta et le commissariat fédéral, vient de publier des lignes directrices sur la gouvernance responsable des données, la protection de la vie privée à un niveau global. C'est la voie de l'avenir. Nous examinons globalement l'entreprise pour vérifier si ses pratiques, ses politiques et ses mécanismes de contrôle, la protection intégrée de la vie privée, par exemple, sont entièrement adéquats.

● (1215)

M. Blaine Calkins: Merci.

Madame Cavoukian, vous voulez ajouter quelque chose?

Mme Ann Cavoukian: Tout d'abord, les utilisateurs et les consommateurs, c'est-à-dire nous tous, nous devons être plus vigilants et dialoguer avec les entreprises dont nous utilisons les services. Cela peut sembler difficile à faire. Facebook est une grosse organisation, n'est-ce pas. Comment pouvez-vous la faire changer? Vous seriez étonné d'apprendre tous les changements que cette entreprise a effectués. Quand elle a adopté sa pratique de protection de la vie privée, ou encore son fil de nouvelles, en 2006, tout le monde a protesté et elle a fait marche arrière. Elle a commis de nombreuses maladresses, et ce sont les pressions du public qui l'ont forcée à rajuster le tir.

Voyons un peu ce que les entreprises peuvent faire, ce que nous pouvons leur demander de faire, et ce que nous pouvons demander au gouvernement aussi. Les appareils portables, nous le savons tous, c'est la voie de l'avenir. Tout le monde s'y met. Pourtant, les documents stratégiques, entre autres, sont muets à ce sujet. Aux États-Unis, on utilise ce qu'on appelle le bouton bleu. Je crois que cela a été créé à l'intention des anciens combattants, pour qu'ils puissent consulter leurs dossiers de santé, ce que le ministère des Anciens combattants possédait à leur sujet. Ils ont ce bouton bleu qui leur donne un accès direct à leur information. On parle maintenant d'appliquer cette idée au secteur de l'énergie avec un bouton vert. Pour connaître votre consommation d'énergie, vous pourriez utiliser un bouton vert. Vous cliquez dessus et vous voyez quelle est votre consommation, vous pouvez la comparer à celle de vos voisins, etc.

Cela montre que les entreprises sont beaucoup plus circonspectes en ce qui concerne l'information qu'elles recueillent automatiquement au sujet des consommateurs, subrepticement ou sans leur consentement. Le contraire de protection implicite de la vie privée, c'est que tout est implicitement public. Il faut renverser cela. Il faut modifier cet état de choses. Les entreprises doivent savoir qu'elles ont des comptes à vous rendre à vous, l'utilisateur, la personne visée par les renseignements. Elles doivent faire preuve de transparence lorsqu'il s'agit de l'information qu'elles détiennent à votre sujet. Vous devez savoir ce qu'elles ont en main. Sinon, vous ignorez quels risques vous courez, en cas de piratage ou d'atteinte à la protection des données.

Linkedln vient d'être victime d'une manoeuvre frauduleuse, et des mots de passe ont été volés. Vous ne savez pas quels renseignements seront accessibles. Il est très important d'avoir cette transparence. Nous devons tous nous plaindre et exercer des pressions sur les entreprises. Comprenez-moi bien, je ne suis pas contre les entreprises. J'adore les entreprises. Ce sont les entreprises dynamiques qui donnent sa vigueur à notre économie. Elles doivent aussi savoir qu'il faut qu'elles protègent leurs clients et les renseignements personnels de leurs clients. Comment peuvent-elles s'y prendre. Nous pouvons les aider à y arriver et à bien communiquer avec leurs clients.

M. Blaine Calkins: Dans le monde des affaires, il est beaucoup question d'acceptabilité sociale. Je crois qu'il faut commencer à parler d'acceptabilité sociale au sujet de ce que les médias sociaux font de nos renseignements personnels.

Mme Ann Cavoukian: Oui, vous avez parfaitement raison.

[*Français*]

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

Je vais donc laisser la parole à M. Andrews, qui dispose de sept minutes.

[*Traduction*]

M. Scott Andrews (Avalon, Lib.): Merci beaucoup. Je vous souhaite la bienvenue, mesdames.

J'ai quatre ou cinq questions à poser, et mes trois premières s'adressent à Mme Denham. Vous avez brièvement parlé...

[*Français*]

Le président: Je vais maintenant donner la parole à M. Tweed, qui invoque le Règlement.

[*Traduction*]

M. Merv Tweed (Brandon—Souris, PCC): Merci.

Monsieur le président, je demande à nos invités et aux membres du comité de me pardonner, mais le député qui a actuellement la parole doit présenter des excuses au comité. Les médias, eux, ont présenté des excuses pour avoir agi de façon inappropriée et enfreint le secret du comité, mardi dernier.

Je donne l'occasion au député de s'excuser maintenant, et nous pourrons alors poursuivre la discussion, ou nous pouvons le faire un peu plus tard. Alors je laisserai d'abord la parole au député pour qu'il s'excuse de son comportement lors de la dernière réunion.

[*Français*]

Le président: Merci.

J'ai bien entendu votre rappel au Règlement.

Je vais donc laisser la parole à M. Angus.

[*Traduction*]

M. Charlie Angus: Je suis désolé de cette grande déclaration destinée à la galerie. Il y a eu une discussion à huis clos, et vous pouvez me rappeler à l'ordre pour cela si vous le voulez. À ce moment-là, nous nous étions engagés à en discuter un peu et à présenter une recommandation au comité. Malheureusement, M. Del Mastro a fait une déclaration publique à la Chambre. Et voilà que vous utilisez cet incident dans le contexte d'une réunion télévisée pour faire une déclaration vous aussi.

Nous nous étions entendus au sein du comité et nous devions formuler des recommandations. Je crois que vous essayez seulement de l'embarrasser.

Selon moi, M. Andrews devrait attendre que nous reprenions la conversation de mardi dernier.

● (1220)

[*Français*]

Le président: Je vais laisser M. Andrews décider de ce qu'il veut faire. S'il tient à continuer la discussion avec les témoins et à revenir à ce sujet un peu plus tard, comme le prévoit l'ordre du jour, nous pouvons en rester là.

Monsieur Andrews, vous pouvez continuer.

[*Traduction*]

M. Scott Andrews: Avant de démarrer l'horloge, nous devrions peut-être discuter de cela en public, quand nos témoins seront partis, et je suis parfaitement disposé à répondre aux commentaires de M. Tweed à ce moment-là. Je préférerais ne pas le faire à huis clos, comme cela est suggéré dans notre ordre du jour. J'en parlerai plus tard.

Puis-je poursuivre mes questions?

[*Français*]

Le président: Oui. Vous disposez de sept minutes.

[*Traduction*]

M. Scott Andrews: Merci.

Madame Denham, j'ai trois questions à vous poser. M. Calkins vient de parler de connaissance et de consentement, et vous avez mentionné la nécessité de limiter l'utilisation des renseignements recueillis. Avez-vous des suggestions à nous présenter quant à la façon dont nous pouvons réglementer cet aspect? Comment pouvons-nous limiter l'utilisation des renseignements que ces entreprises recueillent?

Ma deuxième question est la suivante: vous avez parlé d'enquêtes, vous en avez mentionné une. Combien d'enquêtes avez-vous menées, et est-ce qu'elles portaient sur les entreprises de médias sociaux? Je crois que dans votre exemple ce n'était pas une entreprise de médias sociaux mais un tiers qui utilisait l'information. Mais je me trompe peut-être.

Vous avez notamment dit avoir formulé des lignes directrices à l'intention de ce groupe de l'extérieur. Je me demande si vous pourriez nous les communiquer. Est-ce qu'elles étaient très détaillées? Pourriez-vous nous préciser un peu tout cela?

Mme Elizabeth Denham: Certainement.

Pour ce qui est de limiter l'utilisation que les entreprises de médias sociaux font des renseignements, évidemment les utilisateurs inscrivent volontairement ces renseignements dans leurs profils. L'entreprise ne devrait les utiliser qu'à des fins qui ont été clairement exposées. C'est cela, le principe de la transparence.

Si l'entreprise veut utiliser les renseignements à d'autres fins, elle doit d'abord en demander l'autorisation aux utilisateurs et leur fournir des explications. Cet aspect est très bien illustré dans le cas de Facebook. Vous êtes un utilisateur de Facebook, et voilà que Facebook déploie un logiciel de reconnaissance faciale. C'est une utilisation inédite des données, une utilisation plus spécifique. Et cette nouvelle utilisation pourrait mener à un détournement de fonction. Je crois que dans ce cas l'entreprise doit expliquer aux utilisateurs les nouvelles utilisations, les nouveaux gadgets qui sont offerts, et obtenir leur consentement.

Cela est très important. Si de nouveaux partenaires interviennent, si le nombre d'applications de tiers qui utilisent les données augmente, l'utilisateur doit en être informé et pouvoir facilement refuser ou contrôler l'utilisation de ses renseignements.

Votre deuxième question portait sur le nombre d'enquêtes réalisées sur des sites de médias sociaux par opposition aux enquêtes intéressant les médias sociaux. J'ai cité l'exemple de cette enquête qui portait, tout bien pesé, sur la situation d'emploi et la façon dont les employeurs ou de tierces parties exploitent les médias sociaux. Je voulais attirer votre attention sur cette enquête parce qu'il est important de se demander comment les médias sociaux sont utilisés par les parties à un litige, les policiers, les employeurs, les établissements d'enseignement postsecondaires, puisque cela s'inscrit dans votre étude.

Nous avons réalisé plusieurs de ces enquêtes, et je vous ferai parvenir nos lignes directrices sur le contrôle des références au moyen des médias sociaux. Je les enverrai au greffier.

M. Scott Andrews: Merci beaucoup.

Madame Cavoukian, j'ai une question concernant la protection intégrée de la vie privée. Avez-vous discuté de ce concept avec les entreprises de médias sociaux, Facebook et Google? Est-ce qu'elles ont des opinions à ce sujet?

● (1225)

Mme Ann Cavoukian: J'ai rencontré des responsables de Facebook et de Google, et la protection intégrée suscite certainement un intérêt considérable. Dans le cas de Facebook, je dirais que l'entreprise juge que la protection intégrée de la vie privée est incompatible avec son modèle opérationnel. Ce modèle, c'est l'utilisation d'un maximum de renseignements à toutes les fins possibles, et si les choses vont trop loin — comme cela s'est produit pour le fil de nouvelles — on peut toujours reculer un peu.

J'ai beaucoup de respect pour Mark Zuckerberg. Je lui ai parlé. Il comprend que la question de la vie privée est une question de contrôle et, selon moi, il tient beaucoup à sa vie privée. Mais pour ce qui est du modèle opérationnel, je crois que le concept n'intéresse pas la société.

Google, par contre, est intéressé. Regardez Google+ — c'est le média social de Google —, des efforts ont été déployés pour intégrer des fonctions de protection de la vie privée. Les responsables de Google m'ont invitée à aller discuter de protection intégrée avec leurs ingénieurs principaux, qui étaient en train de concevoir le programme, et leur expliquer comment y parvenir en termes de minimalisation des données et de protection implicite de la vie privée. C'est le concept qui sous-tend les fameux cercles et la volonté de minimiser la collecte de renseignements.

Je ne vais pas trop insister pour faire adopter la protection intégrée de la vie privée. Je crois que les entreprises y viendront d'elles-mêmes, progressivement, si le modèle opérationnel repose sur le recrutement d'un nombre maximal de clients.

Cela dit, il est possible d'utiliser les médias sociaux et de protéger sa vie privée, et je pense ici à l'expérience de Google+ avec les cercles. De nombreuses personnes utilisent cette plate-forme de médias sociaux. J'ignore ce que sont les chiffres maintenant. Je crois qu'il y a plus de 50 ou 60 millions d'utilisateurs, mais il faudra le confirmer. Ce système vous permet de partager de l'information uniquement avec un petit public composé de personnes que vous connaissez.

Si vous me le permettez, monsieur, j'aimerais ajouter un commentaire au sujet de votre première question. Pour minimiser les données et les collectes et respecter la notion de but premier, nous avons, en Ontario, créé un permis de conduire amélioré qui peut remplacer le passeport à la frontière.

Évidemment, il faut pour cela recueillir de l'information. Nous avons inscrit au règlement quels renseignements, quels identificateurs personnels, pouvaient être recueillis: nom, adresse. Nous avons dit qu'il fallait définir les champs avec précision plutôt que de les laisser ouverts. Nous avons sommes parvenus à nos fins. Il est possible de limiter la collecte de renseignements personnels en définissant avec précision et très étroitement ce qui est autorisé.

[*Français*]

Le président: Merci.

Malheureusement, votre temps est écoulé, monsieur Andrews.

Je vais laisser les sept dernières minutes à M. Butt. Le temps file et le comité procédera à ses travaux par la suite.

[*Traduction*]

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

Je remercie infiniment les commissaires de l'Ontario et de la Colombie-Britannique.

Je vais d'abord demander à chacune de vous s'il y a dans la loi provinciale des éléments précis que nous n'avons pas au fédéral et qui pourraient améliorer la protection de la vie privée. Pouvez-vous me donner un ou deux exemples précis de ce que font les provinces et que nous pourrions envisager?

Comme vous le savez, la Chambre étudie un projet de loi qui touche la LPRPDE. Il sera certainement renvoyé un jour à un comité comme le nôtre, où on l'examinera pour tenter de l'améliorer.

Je vous demande à toutes les deux — commençons par la Colombie-Britannique — se vous pouvez proposer des éléments précis au comité afin d'améliorer les lois fédérales en s'inspirant de ce que vous faites.

Mme Elizabeth Denham: Dans la discussion d'aujourd'hui, nous avons mentionné la nécessité d'améliorer la loi. Il faut aussi améliorer la politique. Il faut offrir des encouragements aux intervenants du secteur privé. Il faut éduquer le public, et en particulier les jeunes Canadiens, au sujet de la façon de se protéger en ligne.

Si les entreprises de médias sociaux devaient refuser de respecter la loi canadienne, il nous faudra de très solides mécanismes d'application parce qu'au fond, c'est l'outil essentiel pour assurer la conformité. Nous pouvons publier toutes les lignes directrices imaginables, rencontrer les entreprises, leur proposer des concepts qui permettent de protéger la vie privée, mais au bout du compte il faut parfois quelque chose de plus convaincant. Il nous faut des pouvoirs d'enquête et des mécanismes d'application.

Selon moi, le pouvoir de prendre des ordonnances est un bon point de départ. Je crois aussi que le signalement obligatoire des violations favorise l'investissement dans la protection des renseignements personnels ainsi que dans la sécurité et la sensibilisation.

● (1230)

M. Brad Butt: Madame Cavoukian?

Mme Ann Cavoukian: Merci.

Je suis d'accord avec Mme Denham.

Je peux prendre des ordonnances en Ontario et, croyez-moi, cela est très efficace. Soyons clairs: c'est un dernier recours. Le pouvoir de prendre des ordonnances, c'est le bâton. Nous l'utilisons très peu.

Prenons l'exemple de la Loi sur la confidentialité des renseignements personnels sur la santé, qui s'applique aux organisations de santé des secteurs public et privé en Ontario — des organisations qui sont nombreuses. Cette loi a été adoptée en 2004. J'ai pris seulement 11 ordonnances en vertu de cette loi — c'est-à-dire pendant une période de huit ans environ — parce que les organisations sont fortement encouragées à collaborer avec nous dès le départ, et c'est toujours ce que nous essayons de faire. Nous collaborons. Nous cherchons à régler de façon officieuse les enquêtes et les problèmes, et nous en avons eu des centaines, voire, des milliers. Cela fonctionne très bien. La carotte paraît nettement préférable quand on sait qu'il existe aussi un bâton.

À l'occasion, nous avons dû prendre des ordonnances. Nous ne l'avons pas fait de gaieté de coeur, mais nous savions que c'était nécessaire. Souvent, l'ordonnance est un outil d'éducation. Elle envoie un message très clair quant à la norme en vigueur et à nos attentes à cet égard. Le pouvoir de prendre des ordonnances est donc essentiel.

Nous avons le signalement obligatoire en vertu de la Loi sur la confidentialité des renseignements personnels sur la santé. C'est également une mesure très importante parce qu'elle informe la population de la violation. C'est une garantie d'ouverture et de transparence.

Nous avons aussi, avec la Loi ontarienne sur la modernisation de la réglementation, un outil politique, en quelque sorte, qui permet d'examiner de près la façon dont les solutions de protection ont été intégrées aux activités de réglementation. La collaboration est donc très importante.

Je dois aussi ajouter que mon personnel et moi rencontrons régulièrement des représentants de ces organisations. L'éducation publique est bien sûr très importante, mais il faut aussi rencontrer les organisations qui relèvent de votre compétence pour les aider à mieux comprendre vos attentes et la façon d'intégrer la protection de la vie privée dans leurs pratiques, leurs technologies et leurs activités quotidiennes.

C'est à nous de leur enseigner cela, et nous le faisons régulièrement. Nous pouvons ainsi minimiser le nombre d'ordonnances que nous prenons, mais chacun sait parfaitement que c'est un pouvoir que nous avons. Cela est très important. Cet instrument est très puissant.

M. Brad Butt: En dernier lieu, je vais vous demander de commenter ceci. La commissaire Stoddart nous a parlé de l'information sur le produit du travail, que la commission nationale examine au cas par cas plutôt qu'en fonction d'une définition précise. Pouvez-vous nous expliquer la différence entre la démarche axée sur une définition précise et l'approche du gouvernement fédéral, l'étude des dossiers au cas par cas?

Ma question s'adresse à nos deux témoins.

Mme Elizabeth Denham: Est-ce que vous parlez de la définition applicable à l'information sur le produit du travail dans la LPRPDE?

M. Brad Butt: Oui, je crois.

Mme Elizabeth Denham: Il me paraît important de bien définir le produit du travail pour extraire de la définition de renseignements personnels ce qui peut correspondre uniquement à un produit créé dans le lieu de travail — un avis juridique établi par un avocat, un rapport rédigé par un ingénieur. Selon moi, dans ces cas il ne s'agit pas de renseignements personnels, mais plutôt d'information dérivée du travail et qui ne devrait pas être assujettie à la loi.

Je crois que c'est ce que vous me demandiez?

M. Brad Butt: Oui, merci.

Madame Cavoukian?

● (1235)

Mme Ann Cavoukian: Je suis d'accord avec Mme Denham. Parfois, dans le cadre de votre travail, vous produisez quelque chose qui contient des renseignements personnels, par exemple votre nom et le titre de votre poste, et c'est normal, ce ne sont pas des renseignements personnels aux termes de la loi, parce qu'il ne s'agit pas de vous personnellement. Ces renseignements se rapportent à votre travail et à ce que vous êtes tenu de faire au travail. Il faut donc définir cela et publier cette définition.

Prenez mon cas. Évidemment, je prends des ordonnances, et mon nom figure sur ces documents. Je publie aussi de nombreuses décisions, et mon nom y est attaché. Il serait ridicule de dire qu'il s'agit de renseignements personnels. Évidemment, je suis identifiée, mais c'est en raison du travail que je fais et cela doit être public. Ce n'est pas parce que c'est mon identificateur personnel que ça ne devrait pas être public, si c'est bien votre question. C'est une question de contexte.

[*Français*]

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

Je remercie les deux commissaires qui ont accepté de témoigner et qui nous ont livré des présentations très instructives.

Madame Borg, vouliez-vous invoquer le Règlement?

Mme Charmaine Borg (Terrebonne—Blainville, NPD): En fait, comme nous sommes en communication avec deux témoins très intéressants, nous pourrions peut-être remettre les travaux du comité à la prochaine séance, soit mardi prochain, de façon à pouvoir passer un peu plus de temps avec ces dames.

Le président: Y a-t-il un consentement unanime à ce sujet?

Ça ne semble pas faire consensus.

[*Traduction*]

M. Chris Warkentin (Peace River, PCC): Est-ce qu'il ne faudrait pas réserver un peu de temps? Je sais que M. Andrews voulait faire une déclaration à la fin de la réunion. J'ignore s'il veut procéder de cette façon ou s'il préférerait le faire à la Chambre.

[*Français*]

Le président: C'est à son choix. Nous pourrions continuer pendant quelques minutes et en réserver cinq à la fin pour reparler de ce sujet.

Nous allons donc réserver cinq minutes à la fin de la séance. Selon l'ordre du jour, il va y avoir une période de questions et réponses d'une durée de cinq minutes réservée aux commissaires.

Bref, comme vous êtes très intéressantes, nous allons vous garder un peu plus longtemps avec nous.

Madame Borg, vous disposez de cinq minutes.

Mme Charmaine Borg: Merci beaucoup.

Je suis très heureuse de pouvoir vous poser des questions. Vous disposez d'un bon nombre de renseignements très pertinents dans le cadre de l'étude. En outre, il va être possible de développer des questions comme la façon de protéger nos renseignements personnels dans la base de données et selon des paramètres par défaut favorables à la protection de la vie privée.

Madame Cavoukian, j'aimerais vous poser une question sur les nouvelles technologies.

Vous avez dit être en train de consulter plusieurs ingénieurs à qui vous expliquez comment utiliser les modèles de protection de la vie privée et les intégrer aux nouvelles technologies. D'autres témoins ont dit que certaines technologies recueillaient par accident des données et qu'elles ne permettaient pas la destruction des données.

C'est un peu nouveau, mais j'aimerais savoir comment, au niveau national, les nouvelles technologies qui sont développées pourraient inclure ce modèle de protection intégrée de la vie privée.

[*Traduction*]

Mme Ann Cavoukian: Nous avons divers moyens à notre disposition. Évidemment, nous avons pour tâche de sensibiliser et d'éduquer la population, nous le faisons avec énergie. Sachez que sur la scène internationale on s'intéresse de plus en plus à la protection intégrée de la vie privée. Comme je l'ai dit, ce concept est devenu la norme internationale en 2010. Je vous invite à vous rendre sur le site www.privacybydesign.ca, vous y trouverez une foule d'information à ce sujet.

La majorité des organisations procèdent à des évaluations des facteurs relatifs à la vie privée, des EFRVP, lorsqu'une nouvelle technologie, une nouvelle pratique exemplaire ou un nouveau processus sont adoptés. Vous pouvez exiger ou demander que ce processus reflète la notion de protection intégrée. Je me permets de vous suggérer à nouveau de visiter notre site Web. L'an dernier nous avons réalisé une EFRVP de la protection intégrée de la vie privée, la PIVP. Cette EFRVP a été réalisée justement pour refléter les exigences de la PIVP. C'est un outil essentiel, quelle que soit la pratique. Lorsque vous avez une nouvelle technologie ou une nouvelle pratique opérationnelle, vous effectuez une EFRVP pour pouvoir cerner les risques et les atténuer avant d'instaurer le programme ou la pratique opérationnelle.

En exigeant que les sept principes fondamentaux de la protection intégrée de la vie privée soient reflétés dans l'EFRVP, et donc dans le nouveau programme ou la nouvelle pratique opérationnelle, vous avez au moins la certitude que ces questions seront examinées. Le genre de minimalisation des données dont vous parliez précédemment, pour prévenir l'accès fortuit aux données et leur détournement à d'autres fins, les atteintes découlant de l'utilisation des renseignements à des fins imprévues — tous ces problèmes qui nous inquiètent tant... Tout cela peut se faire dès le départ. C'est ce qu'il y a de bien dans la protection intégrée de la vie privée. Elle tente de dégager les risques d'atteinte à la vie privée dès le début, dès l'apparition de la technologie ou pendant la mise au point du programme.

Si vous intégrez les fonctions de protection au départ, il est beaucoup plus facile de minimiser les atteintes et de les prévenir avant l'opérationnalisation du programme ou de la technologie. Cela fait une grosse différence. Selon moi, l'EFRVP est l'instrument idéal. Nous avons d'ailleurs un CD à ce sujet. Je peux le faire parvenir à tous les intéressés.

Comment faut-il concevoir la protection intégrée de la vie privée? En 2010, quand le concept est devenu la norme internationale, on m'a demandé d'aider certains organismes de réglementation étrangers à l'appliquer. Comment faut-il s'y prendre?

Nous avons mis au point un programme très accessible. Il expose toutes les étapes de mise en oeuvre des principes, la façon de procéder. Je le distribue à tous les intéressés. Nous l'avons distribué à des universités, à Intel et à diverses autres entreprises. Toutes les entreprises de technologie en ont un exemplaire. Essentiellement, il illustre toutes les étapes.

Merci.

● (1240)

[*Français*]

Mme Charmaine Borg: Merci beaucoup.

Nous aimerions bien obtenir une copie de ce CD. Ce serait dans l'intérêt du comité.

Vous n'avez pas eu la chance d'expliquer le fonctionnement du chiffrement biométrique. Pouvez-vous nous expliquer son fonctionnement de façon détaillée? Comment peut-on s'assurer qu'on n'est pas en train de recueillir des données sur tout le monde qui entre dans un édifice ou qui navigue sur un site Web?

[*Traduction*]

Mme Ann Cavoukian: D'accord, avec plaisir. C'est vraiment très simple, malgré les apparences.

Disons que votre photo est prise ou que vos empreintes digitales sont relevées. Normalement, les programmes de reconnaissance faciale ou biométrique saisissent, comme je l'ai dit, ce qu'on appelle un gabarit, une représentation numérique des caractéristiques essentielles de votre visage ou de votre doigt. Ce gabarit est stocké dans la base de données et il est utilisé pour faire des comparaisons.

Le problème se pose, comme je l'ai dit, quand les policiers se présentent munis d'un mandat. Vous devez leur donner accès à la base de données. Ils pourront comparer votre gabarit avec une photo qu'ils ont prise sur les lieux d'un crime, par exemple. S'ils trouvent une correspondance, vos renseignements sont automatiquement utilisés à des fins qui n'avaient jamais été envisagées.

Par contre, le chiffrement biométrique fonctionne différemment. Il utilise les particularités de vos traits ou de votre doigt pour chiffrer ou coder certaines autres données: cela devient un NIP, un numéro alphanumérique impossible à interpréter — c'est parfait. Ce sont ces données chiffrées, ces autres données, qui sont conservées.

Il y a donc deux aspects. Si les policiers se présentent, qu'est-ce qu'ils trouvent? Vous leur ouvrez votre base de données, mais ils n'y trouvent rien parce que votre photo n'y est pas, il est impossible de déchiffrer ce qui se trouve dans la base de données, et l'information n'est donc pas accessible.

C'est très joli, mais que se passe-t-il en cas d'attaque pure et simple? Cela arrive. Il y a toujours un risque de piratage informatique. Si des pirates réussissent à entrer dans la base de données, qu'est-ce qu'ils trouvent? Rien d'important. Ils n'ont pas votre visage ni vos empreintes. Ils ont eux aussi ce chiffre sans signification qui correspond à votre visage ou à vos empreintes et qu'ils ne peuvent pas utiliser. Ils ne trouveront rien d'important. C'est un système qui fonctionne à merveille. Allez sur notre site Web et vous verrez que l'Université de Toronto a collaboré avec OLG pour perfectionner le programme. Ils ont atteint des niveaux sans précédent, en ce qui concerne non seulement la protection de la vie privée, mais aussi la sécurité et la précision, dans le domaine de la biométrie.

Morpho, une grande société basée à Paris, en France, est la principale société de biométrie dans le monde — elle vient d'acheter Sagem, qui était autrefois la plus importante; c'est devenu Morpho. Elle étudie actuellement le chiffrement biométrique en vue de créer un prototype, elle doit lancer un projet pilote à l'automne pour qu'il devienne possible d'incorporer le chiffrement biométrique dans un dispositif. La questions éveille de l'intérêt dans le monde entier. Ce domaine en est encore à ses balbutiements.

Ce qu'il y a de bien, dans l'exemple d'OLG, c'est que tous les clients réguliers des casinos ontariens n'ont aucun souci à se faire lorsque leur image faciale est saisie, au moment où ils entrent au casino. Et je peux vous garantir que les joueurs compulsifs qui veulent qu'on leur refuse l'entrée au casino seront beaucoup mieux servis grâce à ce programme.

Le taux de succès — on parle de taux de rappel — du programme d'auto-exclusion a triplé et même quadruplé. Auparavant, nous pouvions difficilement identifier ces malheureux. Maintenant, le taux de succès est fantastique, et il y a environ 15 000 joueurs compulsifs inscrits au programme à l'échelle de la province. Nous pouvons les aider à faire ce qu'ils nous demandent de faire, soit les exclure, sans empiéter sur la vie privée de quiconque. Nous leur avons également dit que les renseignements qui nous permettent de leur interdire l'entrée des casinos ne peuvent être utilisés à aucune autre fin — il n'y a aucune utilisation secondaire.

● (1245)

[*Français*]

Le président: Merci. Je vais devoir vous arrêter pour laisser le dernier temps de parole de cinq minutes à M. Calkins.

[*Traduction*]

M. Blaine Calkins: Merci beaucoup, monsieur le président. C'est la journée de Blaine Calkins au comité, aujourd'hui.

Madame Cavoukian, parlez-nous un peu plus de ce gabarit numérique. Il me semble que c'est une clé de chiffrement, en quelque sorte. Est-ce que je comprends bien?

Mme Ann Cavoukian: Dans le chiffrement biométrique, la clé serait en fait l'image faciale ou le doigt. Vos caractéristiques personnelles deviennent en effet l'équivalent d'une clé de chiffrement que vous utilisez pour chiffrer certaines données.

M. Blaine Calkins: Mais cette clé, pour qu'on puisse lire les données quand on en a besoin, il faut la connaître. Alors quel serait le multiplicateur pour cette clé? L'algorithme serait...

Mme Ann Cavoukian: La clé de déchiffrement, c'est votre visage ou votre doigt. Les données biométriques constituent la clé de déchiffrement.

C'est la raison pour laquelle, si les policiers se présentent dans les bureaux d'OLG, OLG peut les laisser consulter sa base de données. Ils n'ont pas de clé de déchiffrement. Ces clés, ce sont les images faciales des participants au programme.

M. Blaine Calkins: C'est bien. Et cela fait doublement réfléchir quand on dit qu'il ne faut pas perdre la clé! J'imagine que nous devrons faire preuve d'une certaine prudence. Je suis heureux d'apprendre que mon image faciale n'a aucune valeur. Je sais que vous ne vouliez pas dire cela. Je plaisante, évidemment.

Je vous remercie de cette explication. Je comprends parfaitement. C'est ainsi que je pensais que les choses fonctionnaient.

Je veux aborder la question de la destruction de l'information. J'ai été administrateur d'une base de données Oracle. Que la base de données soit relationnelle ou orientée objets, les données sont stockées sous diverses formes, selon le système utilisé. Très souvent, dans les interfaces utilisateur, des renseignements sont recueillis, et il nous arrive aussi de demander que nos renseignements soient exclus d'une base de données. La différence entre désactivation et destruction n'est pas négligeable. En effet, nous pouvons simplement désactiver un dossier, et il peut alors sembler que la personne n'est plus un client de l'entreprise, mais en fait les données des dernières transactions se trouvent encore dans la base de données.

Nous pouvons être tenus de conserver ces renseignements aux fins de l'impôt, par exemple, pour des raisons juridiques ou légales. Mais parfois, dans le cadre de certaines transactions, quand une personne renonce à protéger ses renseignements personnels pour pouvoir utiliser un logiciel libre sur son appareil portable, les choses sont complètement différentes.

Je me demande si vous, madame Cavoukian, ou vous, madame Denham, pouvez nous dire ce que vous faites quand un utilisateur ou un citoyen demande que des renseignements soient supprimés. Que peut-on faire pour protéger ces Canadiens?

● (1250)

Mme Elizabeth Denham: C'est une question très importante. Le droit de se faire oublier est un aspect fondamental de la protection de la vie privée. Nos lois permettent donc aux organisations de conserver les renseignements seulement dans la mesure où elles en ont encore besoin à des fins commerciales. Ensuite, elles doivent les supprimer.

J'ai mené une enquête sur Facebook en 2009, au commissariat fédéral, et c'était vraiment un des grands problèmes que nous avons relevé. Nous avons constaté des différences considérables entre désactivation d'un compte et suppression des données. La commissaire fédérale a recommandé de prendre des mesures pour que les clients puissent facilement supprimer leurs comptes et qu'on leur explique clairement la différence entre désactivation, c'est-à-dire le fait de placer les données hors ligne au cas où l'utilisateur changerait d'idée et voudrait revenir à Facebook, et la suppression — et dans ce cas, si je ne me trompe pas, il faut compter 30 jours avant que toutes les données soient supprimées.

Nous voulions que l'entreprise permette vraiment aux utilisateurs de choisir facilement une de ces options et qu'ils puissent vérifier si leur décision a effectivement été respectée.

Revenons au pouvoir de prendre des ordonnances. La commissaire fédérale est un ombudsman et elle peut formuler des recommandations. Ma collègue Ann Cavoukian et moi-même, par contre, avec notre pouvoir de prendre des ordonnances, nous pouvons ordonner à une entreprise de supprimer les données, et il faut alors que cela soit fait dans les 30 jours. La loi provinciale fixe ce délai à 30 jours. C'est un instrument très puissant.

Mme Ann Cavoukian: Merci, madame Denham. Comme vous, nous avons le pouvoir de prendre des ordonnances et nous pouvons ordonner à une entreprise de ne plus recueillir certains renseignements ou de détruire des renseignements personnels qui ont été recueillis en contravention de la loi.

C'est ce que j'ai fait, il y a quelques années, et croyez-le ou non cette ordonnance visait le service de police d'Ottawa. Les policiers avaient recueilli des renseignements dont j'ai ordonné la destruction. J'ai eu le plaisir de rencontrer Vern White, qui était à l'époque chef de la police d'Ottawa et qui est aujourd'hui sénateur.

Nous avons donc, dans notre sphère de compétence, la capacité d'ordonner la suppression de renseignements. Nous pouvons ensuite demander que des vérifications soient effectuées par des tiers, pour confirmer que les données ont bel et bien été supprimées, mais je suis convaincue que la police d'Ottawa l'a fait.

Comme l'a mentionné Mme Denham, le droit de se faire oublier est extrêmement important. Il figure en bonne place dans le nouveau règlement sur la protection des données que l'UE est en train de rédiger.

Cet aspect est en outre de plus en plus important, compte tenu du peu de contrôle que vous exercez en matière d'accès dans les médias sociaux et sur d'autres tribunes en ligne. Est-ce que les données ont vraiment été supprimées? Ont-elles été désactivées? Pendant combien de temps...? Quelles garanties avons-nous?

Je crois que vous avez très peu de garanties, pour ne pas dire aucune, en ce qui concerne l'information recueillie par le secteur privé et qui échappe à ma compétence ou à celle d'autres autorités. Même notre fonction de vérification est difficile à assurer. Il faut vraiment faire des efforts. La FTC et d'autres organisations cherchent actuellement à intégrer l'obligation de vérification par un tiers, de sorte que si l'on ordonne la suppression de dossiers, il sera possible de le vérifier.

Je veux toutefois vous signaler une chose, et ce sera mon dernier commentaire. À l'avenir, selon moi, la situation sera de plus en plus difficile si les entreprises et les gouvernements n'adoptent pas la protection intégrée de la vie privée pour offrir de façon proactive la fonction implicite de protection de la vie privée. Vous ne pourrez jamais être certain que vos dossiers sont protégés ou qu'ils ont été supprimés. Ce domaine deviendra une véritable jungle.

Nous travaillons de concert avec l'Université de Toronto pour mettre au point un nouveau concept appelé SmartData. Sur notre site Web, vous constaterez que nous venons de tenir un symposium international sur le concept SmartData, c'est-à-dire l'élaboration d'outils virtuels pour la personne visée par les renseignements, des outils qui vous serviront d'agent virtuel pour protéger vos renseignements et agir en votre nom d'une façon contextuelle.

Je crois que j'ai assez parlé. Je voulais simplement mentionner l'existence de ce projet SmartData. Vous pouvez visiter notre site Web, mais nous pouvons aussi vous faire parvenir l'information. C'est ce que nous appelons la protection intégrée — donner au consommateur, aux utilisateurs, des outils qui leur permettent de protéger leurs renseignements.

Merci.

● (1255)

[*Français*]

Le président: Merci. Je vous remercie une deuxième fois d'avoir été disponibles aujourd'hui pour vos présentations.

J'espère qu'on pourra avoir accès au document dont vous avez parlé, madame Cavoukian et que, par l'entremise du greffier, on pourra le transmettre à chaque membre du comité. Je vous remercie d'avoir été ici.

On va suspendre la séance pendant quelques minutes et revenir ensuite, pour les cinq dernières minutes, afin de parler des travaux du comité, comme vous le savez.

Merci.

● (1255)

(Pause)

● (1255)

Le président: Nous reprenons la séance.

M. Andrews voulait vous dire quelques mots.

[*Traduction*]

M. Scott Andrews: Merci, monsieur le président.

Comme mes collègues le savent, j'ai présenté des excuses à huis clos lors de notre dernière réunion et je le ferai pendant la partie publique de la réunion d'aujourd'hui. C'est pour cette raison que j'ai demandé que nous poursuivions notre réunion en public.

Je présente mes excuses.

[*Français*]

Le président: M. Andrews s'est excusé ici, en public.

Y a-t-il autre chose à l'ordre du jour des travaux du comité dont on voulait discuter?

Pour ma part, je voulais faire quelques annonces. J'ai notamment déposé le rapport de la Société du Vieux-Port de Montréal, ce matin. Il a donc été déposé à la Chambre.

La correction qu'on voulait apporter au rapport sur le lobbying a aussi été faite. Elle a été acceptée à la Chambre par consentement unanime. C'est ce que j'avais à vous dire.

Mme Borg voulait-elle ajouter quelque chose?

[*Traduction*]

M. Charlie Angus: Pour faire un suivi de ce qui s'est passé...

Mme Charmaine Borg: D'accord.

M. Charlie Angus: Désolé.

Parce qu'il y a eu deux incidents l'autre jour, et je me demande ce qu'il en est du protocole avec les médias. Ce qui est arrivé à M. Andrews pourrait arriver à n'importe qui, il suffit d'une distraction. Vous vous concentrez sur quelque chose, et quelqu'un arrive par derrière et vous pose une question. Cela m'inquiète.

Cela aurait pu être... Vous savez les médias n'y ont peut-être pas porté attention, mais est-ce que nous n'avons pas un protocole qui précise le rôle, les limites des journalistes qui s'approchent de la table quand nous travaillons?

Parce que je crois qu'il nous faut prendre une position claire — quand le comité de l'éthique est en réunion, les journalistes ne devraient pas pouvoir venir poser ainsi des questions aux députés, au dépourvu. Je crois qu'il nous faut une sorte de... Il n'est pas nécessaire de faire de grandes déclarations, mais nous devrions nous entendre clairement sur la façon dont nous pouvons travailler ensemble.

[*Français*]

Le président: Le greffier me mentionne que certaines règles qui existent déjà sont censées encadrer le travail des journalistes en comité. Je vais lui céder la parole.

[*Traduction*]

Le greffier du comité (M. Chad Mariage): Merci, monsieur le président.

En février 2009, un protocole d'entente entre la tribune de la presse parlementaire et la Chambre des communes a été conclu. Il était fondé sur un rapport initial et un essai qui avait été mené à la suite d'une étude réalisée par le Comité de la procédure et des affaires de la Chambre.

Je peux distribuer cette directive aux députés, si vous le désirez.

[*Français*]

Le président: Monsieur Harris, vous avez la parole.

[*Traduction*]

M. Richard Harris (Cariboo—Prince George, PCC): J'aimerais avoir une précision. Je crois que dans le protocole il est interdit qu'un journaliste, un représentant de la presse, vienne interrompre un député qui participe à une séance du comité. C'est bien cela?

Si tel est le protocole — et les journalistes qui travaillent régulièrement sur la Colline le connaissent certainement —, la journaliste qui s'est approchée d'un député a enfreint le protocole. Qu'elle ait pris le député au dépourvu ou pas, elle porte certainement une part de responsabilité.

Si la journaliste a enfreint le protocole, le comité serait parfaitement justifié soit de se plaindre par l'entremise du président soit de rappeler directement à la journaliste l'existence de ce protocole et de lui demander de veiller à ce que cela ne se reproduise pas.

[*Français*]

Le président: Monsieur Butt, voulez-vous ajouter quelque chose?

[*Traduction*]

M. Brad Butt: C'est essentiellement ce que je disais. Je crois qu'il y a une règle actuellement au sujet des journalistes qui voudraient s'approcher de la table du comité pendant une séance. Cela est strictement interdit. C'est ainsi que je l'interprète, et c'est ainsi que les choses doivent être.

La journaliste aurait dû le savoir. Je crois qu'elle a pris M. Andrews au dépourvu, et selon moi c'est malheureux. Je suis d'accord avec M. Harris, la journaliste a une large part de responsabilité. Elle n'est pas nouvelle. Elle est ici depuis un bon bout de temps, alors elle connaît les règles.

Personne ne conteste cette règle. Vous n'approchez pas de la table du comité pendant une séance, un point c'est tout.

● (1300)

[*Français*]

Le président: J'aimerais ajouter que, normalement, on ne permet pas aux journalistes d'être autour de la table quand une séance en cours est publique. On pourrait peut-être rappeler les règles par l'entremise du président de la Tribune de la presse parlementaire, de la Chambre des communes. On pourrait leur rappeler les règles, monsieur Andrews.

[*Traduction*]

M. Scott Andrews: Il serait utile que le comité ait un exemplaire de ces règles. Je crois que vous avez parlé d'un document.

Et vous aussi, vous avez mentionné quelque chose.

Je ne pense pas l'avoir jamais vu. J'aimerais l'examiner.

[*Français*]

Le président: On peut le distribuer immédiatement ou par courriel, si vous voulez.

Monsieur Angus, vous avez la parole.

[*Traduction*]

M. Charlie Angus: Je veux ajouter encore une chose. Vous avez le maillet. Vous maintenez l'ordre. Que nous décidions de publier une déclaration...

J'ignore s'il nous faut aller plus loin. Il y a eu une infraction. Je ne pense pas que ce soit quelque chose qui... Cela aurait pu avoir des conséquences, mais je ne sais pas si nous voulons vraiment pousser plus loin.

Que le président rédige quelque chose ou qu'il fasse une déclaration pour dire qu'à partir de maintenant il en sera ainsi, qu'à notre comité cela ne se fait pas, il suffit de l'inscrire au compte rendu pour que tous en soient conscients, pour que l'on sache que le président s'est prononcé à ce sujet.

[*Français*]

Le président: Si j'ai l'accord du comité, évidemment, je pourrai écrire une déclaration à envoyer à la Tribune de la presse parlementaire pour lui signaler le problème par rapport à ce qui est arrivé. Je pourrais faire approuver cette déclaration par le comité avant de l'envoyer.

Monsieur Calkins, vous avez la parole.

[*Traduction*]

M. Blaine Calkins: Je ne sais pas s'il cela est vraiment nécessaire.

Je crois que la journaliste a présenté des excuses. Elle a admis sa responsabilité et reconnu avoir manqué à ses devoirs. Elle s'est excusée. Cela me suffit.

M. Andrews a lui aussi présenté des excuses pour le même incident.

Cela est malheureux, mais selon moi tous ceux qui suivent ce dossier comprennent maintenant clairement la conduite à tenir à l'avenir.

Je serais heureux que nous passions à autre chose.

[*Français*]

Le président: Je crois qu'il y a un accord pour en rester là. Comme M. Calkins l'a mentionné, à l'avenir, les journalistes feront peut-être un peu plus attention. Cela aura donné une leçon à tout le monde.

Madame Block, vous avez la parole.

[*Traduction*]

Mme Kelly Block (Saskatoon—Rosetown—Biggar, PCC): Je sais que la séance tire à sa fin, mais en tant qu'invitée, aujourd'hui, je me demande s'il ne vaudrait pas la peine de transmettre aussi ce document aux autres comités. Ils ne connaissent peut-être pas cette règle que vous avez dû appliquer ici.

Nous pourrions le mentionner aux autres comités, et s'ils le désirent le document pourrait leur être distribué.

[*Français*]

Le président: Ce pourra certainement être fait par le greffier qui a ce document. Il pourra contacter la haute gestion de tous les greffiers de tous les comités pour s'assurer que les règles sont claires et sont transmises le plus efficacement possible à tous les députés et aux journalistes, qui doivent aussi être au courant.

Y a-t-il autre chose à l'ordre du jour?

Il est déjà 13 h 4. La séance est levée.