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 059 • 1re SESSION • 41e LÉGISLATURE

TÉMOIGNAGES

Le mardi 11 décembre 2012

Président

M. Pierre-Luc Dusseault

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

Le mardi 11 décembre 2012

● (1530)

[*Français*]

Le président (M. Pierre-Luc Dusseault (Sherbrooke, NPD)): À l'ordre, s'il vous plaît.

Nous allons débuter la séance nº 59 du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique en vue de poursuivre l'étude sur la vie privée et les médias sociaux.

Aujourd'hui, nous avons la chance d'avoir deux témoins. En premier lieu, nous aurons un représentant de BlueKai, soit M. Chapell, qui va nous faire une présentation de dix minutes. Par la suite, nous pourrons lui poser des questions. Nous aurons également la commissaire à la protection de la vie privée qui nous rendra visite pour une deuxième fois. Elle nous donnera un résumé de ce qui a été dit jusqu'à maintenant puisque ce devrait être la dernière rencontre sur cette étude.

Sans plus tarder, je laisse la parole à M. Chapell pour dix minutes. Comme je l'ai dit précédemment, nous aurons ensuite l'occasion de lui poser des questions.

Monsieur Chapell, la parole est à vous et je vous remercie de votre présence.

[*Traduction*]

M. Alan Chapell (conseiller juridique externe, responsable de la protection de la vie privée, BlueKai Inc.): Merci, monsieur le président.

Monsieur le président, mesdames et messieurs les membres du comité, je vous remercie d'avoir invité BlueKai à témoigner à cette audience importante, qui vient à point. Je m'appelle Alan Chapell et je suis conseiller juridique externe et responsable de la protection de la vie privée pour BlueKai Incorporated, une société de données numériques dont le siège social est situé à Cupertino, en Californie.

C'est pour moi un honneur de comparaître devant ce comité. C'est avec grand plaisir que je vais vous décrire les activités de BlueKai et faire part au comité des mesures innovatrices que nous avons mises en place au sein de l'entreprise pour protéger les renseignements personnels.

La mission de BlueKai est de créer la première plateforme d'entreprise complète de marketing axé sur les données avec le plus grand souci possible de protection de la vie privée des consommateurs. Nous offrons une plateforme de gestion des données qui permet aux publicitaires de recueillir, de stocker et d'utiliser des données anonymes sur les préférences des consommateurs. Depuis sa fondation, en 2007, BlueKai s'efforce de mettre en application les idéaux de la protection intégrée de la vie privée dont fait la promotion la commissaire à l'information et à la protection de la vie privée, Ann Cavoukian. Nous reconnaissons l'importance d'intégrer la protection de la vie privée à nos produits et services et favorisons une culture de protection de la vie privée des consommateurs depuis notre premier jour.

La plateforme de BlueKai permet aux entreprises d'utiliser des données pseudonymes ponctuelles en matière de marketing à des fins d'analyse et de publicité comportementale en ligne. Elle permet aux entreprises de créer des publics cibles établis en fonction de leurs propres données et de données tierces afin d'atteindre leurs publics cibles grâce à des réseaux de publicité et à des échanges avec des tiers. Elle aide également les entreprises à déterminer avec précision quel type de campagne mener pour mieux cibler les achats dans les médias et trouver des idées de publicité créatives.

Les données de marketing stockées dans la plateforme de gestion des données sont généralement régies par les politiques de nos clients en matière de protection de la vie privée. BlueKai propose des lignes directrices pour aider ses clients à comprendre les lois et les normes d'autoréglementation qui s'appliquent en matière de protection de la vie privée.

BlueKai offre également un service d'échange de données afin de permettre aux entreprises d'utiliser les données pseudonymes de tierces parties dans leurs campagnes de publicité numériques. Nous prenons des mesures pour veiller à ce que les données de marketing des tierces parties accessibles grâce à l'outil d'échange de BlueKai respectent les lois et les normes d'autoréglementation applicables en matière de protection de la vie privée ou qu'elles soient encore plus rigoureuses.

BlueKai a un représentant au conseil d'administration de la Network Advertising Initiative, une coalition de plus de 95 grandes sociétés de publicité en ligne déterminées à élaborer et à mettre en application des méthodes responsables de protection de la vie privée pour régir les comportements publicitaires en ligne. Nous faisons également partie de la Digital Advertising Alliance, le programme d'autoréglementation de l'industrie sur la publicité comportementale en ligne. Depuis notre création, nous participons activement au mouvement d'autoréglementation de la publicité comportementale en Amérique du Nord, en Europe et dans le reste du monde.

Nous savons qu'il y a un programme similaire qui se prépare au Canada pour favoriser l'autoréglementation de la publicité comportementale. Les exigences en matière de protection de la vie privée qui sous-tendent ce programme sont généralement conformes à la position de principe sur la publicité comportementale en ligne du Commissariat à la protection de la vie privée du Canada. Depuis toujours, BlueKai, est un leader de l'autoréglementation de l'industrie. Nous espérons poursuivre nos efforts en ce sens et être l'une des premières entreprises à participer à l'initiative d'autoréglementation canadienne dès qu'elle sera lancée.

J'ajoute enfin que BlueKai participe activement au groupe de travail du Consortium du World Wide Web sur la protection contre le pistage, en vue d'élaborer une norme de non-pistage qui serait intégrée aux navigateurs.

En plus de participer activement aux mesures d'autoréglementation de l'industrie sur la publicité comportementale en ligne, BlueKai a toujours fait preuve de beaucoup d'innovation en matière de protection de la vie privée. J'aimerais présenter deux de ces innovations au comité aujourd'hui.

La première est le registre de BlueKai. BlueKai a été l'une des premières sociétés de marketing numérique à faire véritablement preuve de transparence envers les consommateurs en leur donnant accès à ses données de marketing par le registre BlueKai. Ce registre, qu'on peut consulter à l'adresse BlueKai.com, est gage de transparence pour les consommateurs. Il leur permet de voir quelles préférences sont stockées par les témoins BlueKai sur leur ordinateur.

De plus, les consommateurs peuvent gérer leur profil anonyme en modifiant leurs sujets d'intérêt. Nous croyons fermement que ce degré de transparence envers les consommateurs et ces mécanismes de contrôle contribuent à renforcer la confiance des consommateurs. Nous le constatons dans la pratique; relativement peu de consommateurs qui consultent le registre BlueKai nous demandent de ne plus utiliser leurs données de préférence. Cela nous porte à croire que les consommateurs qui comprennent les façons de faire de BlueKai s'en inquiètent généralement moins.

● (1535)

La deuxième innovation de BlueKai, c'est son outil de protection de l'option de retrait. Il n'est pas évident d'offrir une option de retrait dans un contexte de publicité en ligne parce que les témoins ont deux fonctions. C'est-à-dire qu'ils servent à stocker les données de marketing et à enregistrer l'option de retrait de l'internaute.

Quand les internautes suppriment tous leurs témoins, ils risquent de supprimer en même temps leur option de retrait. Le Commissariat à la protection de la vie privée du Canada est d'avis que l'option de retrait convient à la plupart des formes de publicité comportementale en ligne; cependant, il recommande également que cette option demeure toujours accessible. Cette recommandation est conforme aux recommandations des législateurs du monde entier. Pour suivre ces recommandations, BlueKai a créé l'outil de protection de l'option de retrait.

À l'aide d'un code source ouvert, BlueKai a développé un module externe de navigation Firefox conçu pour protéger l'option de retrait de l'internaute, même quand il supprime ses témoins Internet. La Network Advertising Initiative a reçu l'autorisation d'utiliser ce code, de sorte que toutes les entreprises qui en sont membres peuvent elles aussi recourir à la technologie de protection de l'option de retrait. Ce concept a été repris par la Digital Advertising Alliance et a été élargi pour s'appliquer à la plupart des grands navigateurs Web.

Nous sommes fiers de pouvoir dire que notre travail acharné a permis à BlueKai et à d'autres entreprises de publicité comportementale en ligne de protéger les choix des consommateurs en matière de confidentialité. Nous prenons la protection de la vie privée très au sérieux chez BlueKai et sommes heureux d'avoir eu l'occasion de faire part de nos mesures novatrices dans le domaine à ce comité.

Je suis maintenant prêt à répondre à vos questions.

[*Français*]

Le président: Je vous remercie.

Sans plus tarder, je vais laisser la parole à M. Angus, pour sept minutes.

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

[*Traduction*]

Je vous remercie beaucoup d'être avec nous aujourd'hui. Nous apprécions sincèrement votre participation à cette étude.

Comme vous le savez probablement, nous essayons de dresser un portrait juste de l'univers des grosses données et de leur utilisation dans les médias sociaux, pour que nos recommandations futures ne donnent pas lieu à des dispositions réactives qui nuiraient au développement de nouveaux débouchés. En tant que députés, qui sont loin de maîtriser les connaissances les plus pointues, nous voulons également faire de notre mieux pour nous doter de normes de protection, particulièrement pour protéger la vie privée des citoyens canadiens.

J'aimerais vous poser une première question. BlueKai recueille-t-elle des données sur les Canadiens?

M. Alan Chapell: Nous avons des activités au Canada. Ce n'est pas la part du lion dans nos activités actuellement, mais nous recueillons des données sur les Canadiens.

M. Charlie Angus: Merci.

Nous avons rencontré des représentants d'Acxiom la semaine dernière. Ils nous ont dit que notre marché était trop petit, ce que nous n'avons pas pris personnellement. En règle générale, nous nous sommes plutôt sentis soulagés, je crois, de savoir qu'ils ne s'intéressaient qu'à nos annuaires.

L'un de vos membres fondateurs, Omar Tawakol, je pense...

M. Alan Chapell: Oui: Omar Tawakol.

M. Charlie Angus: Il a dit: « En ce moment, les données ressemblent à de la matière noire et gluante. Le pétrole a été à la révolution industrielle ce que les données sont à notre économie de l'information. »

Faites-vous l'extraction de cette matière noire et gluante ou sa transformation? Quel est votre rôle par rapport à ces données gluantes?

M. Alan Chapell: Je pense qu'il utilise cette analogie pour dire que les données peuvent être très précieuses. Elles peuvent aider beaucoup les consommateurs. Elles peuvent favoriser l'innovation.

Notre principale sphère d'activité, c'est la plateforme de gestion des données, qui se trouve à être la plomberie des pipelines pétroliers, si l'on veut reprendre la même analogie.

M. Charlie Angus: Est-ce que vous mettez les données ponctuelles en commun pour dresser des profils ou prenez-vous les données telles quelles, pour y trouver du sens?

M. Alan Chapell: Je dirais que nous faisons un peu des deux. Il est clair que nous faisons des analyses, c'est une partie intégrante de la plateforme, et le produit d'échange de données nous permet de recueillir des données sur les préférences des consommateurs.

M. Charlie Angus: Très bien.

J'aimerais en savoir un peu plus sur les options de retrait et la question des témoins. Je désactive mes témoins, mais parfois, cela m'empêche d'accéder à un site Web, dans Firefox ou d'autres navigateurs. Je dois donc réactiver mes témoins, ce qui signifie que j'autorise le pistage de mes activités. Je n'ai pas vraiment l'impression d'y avoir donné mon accord; j'ai accepté d'accéder à un site Web et je devais activer mes témoins pour cela. Quelle est l'importance des témoins pour suivre ce que je fais en ligne?

● (1540)

M. Alan Chapell: Les témoins sont essentiels pour toutes sortes de choses en ligne: ils permettent évidemment de faire un pistage, mais ils permettent également au navigateur de mettre des informations en mémoire sur une page X, quand l'internaute la consulte, pour établir ce qu'on appelle un « état » quand l'internaute passe à la page suivante, afin d'assurer une certaine continuité à l'internaute dans sa navigation.

M. Charlie Angus: Cela signifie que si je passe d'un site à un autre, puis à un autre encore, il est possible de me suivre et de dire que je suis passé par ici, par là, puis par là. Il y a une suite qui se dessine.

M. Alan Chapell: C'est tout à fait possible. Cela porterait à croire que la même entreprise a laissé des témoins sur le premier site que vous avez consulté, puis sur le second site, et qu'elle a laissé d'autres témoins encore sur le troisième site que vous avez consulté.

M. Charlie Angus: Mais un courtier en données pourrait tirer l'information de trois endroits différents et établir les liens entre elles. Ce ne serait pas nécessairement le témoin sur Amazon ou un autre site commercial qui les fournirait, mais ces données ponctuelles peuvent être mises en commun pour dresser un profil.

M. Alan Chapell: Je pense que les données ponctuelles peuvent être mises en commun, pas nécessairement pour dresser un profil continu parce que vous avez consulté les sites X, Y et Z, mais si le site X est un site de finances, il est très possible qu'il y ait une indication que le navigateur a accédé à un site Web de finances. Si le site suivant est un site de voyage, il est à tout le moins possible qu'un témoin indiquant une préférence pour le voyage soit laissé dans le navigateur par la suite.

M. Charlie Angus: J'ai lu un article très intéressant dans le *New York Times* sur BlueKai. Il y était écrit:

> Le modèle d'affaire de BlueKai se fonde sur l'idée que nos profils numériques sont anonymes au moment où ils sont vendus aux enchères. En fait, les ordinateurs peuvent lier nos profils numériques à nos véritables identités de manière si précise qu'il sera bientôt difficile de prétendre avec crédibilité que les profils sont anonymes.

Selon ma propre expérience, si je consulte la page d'un conseiller financier, puis que j'essaie de trouver un endroit où aller à Cuba et que je me demande ensuite combien de bouteilles d'alcool acheter pour un party de Noël et que je cherche des prix, il ne s'agit pas de données anonymes. Il est assez facile de faire le lien entre elles et moi, en tant que personne, n'est-ce pas?

M. Alan Chapell: Je dois vous dire d'abord que BlueKai ne fait pas de profilage sur la consommation d'alcool, il est très important de le souligner clairement.

M. Charlie Angus: Dieu merci.

M. Alan Chapell: Il y a un certain nombre de segments qui dépassent les limites d'après nous.

M. Charlie Angus: Mais vous fournissez ce profilage, et il est transmis à une vraie personne. Il ne s'agit pas que de données regroupées.

M. Alan Chapell: Il est envoyé à un navigateur Internet précis...

M. Charlie Angus: Je vois.

M. Alan Chapell: ... qui peut se rapporter ou pas à une personne en particulier, car les ordinateurs ou les navigateurs Internet sont partagés.

M. Charlie Angus: Nous avons reçu des représentants de Google et ils nous ont dit qu'avec leur nouvelle plateforme Chrome — que je n'ai pas encore utilisée, car elle ne fonctionne pas sur mon ordinateur Mac, mais c'est une autre histoire — ils permettent, au fond, un fonctionnement discret complet. En quoi cela influe-t-il sur BlueKai, si les navigateurs commencent à donner aux utilisateurs la capacité d'aller sous la surface sans être détectés? Est-ce que cela influera le moindrement sur votre plan d'affaires?

M. Alan Chapell: La plupart des principaux navigateurs ont offert un type de fonctionnement discret pendant quelques années. Je crois que certains l'appellent « incognito ». Je crois que chaque navigateur a son propre terme pour le désigner. Ils existent depuis un certain nombre d'années. Dans la mesure où ils donnent aux utilisateurs le réconfort de penser que ces séances de navigation Internet seront assujetties aux règles incognito, je pense que c'est une bonne chose. À ce jour, nous n'avons pas remarqué que le fonctionnement discret ou incognito avait une incidence importante sur les affaires de BlueKai.

[*Français*]

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

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

[*Traduction*]

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

Je vous écoute parler de votre plateforme avec grand intérêt. En parlant, vous avez répondu à deux ou trois de mes questions.

J'aimerais parler un peu des témoins. Juste pour être certaine, votre entreprise est bien un agrégateur de données, non?

M. Alan Chapell: Je crois que c'est une description juste.

M. Blaine Calkins: Alors vous utilisez les renseignements regroupés et vous fournissez de la publicité faite par des tiers axée sur un ordinateur en particulier en fonction des témoins qui se trouvent dans la cache ou dans le fichier témoin qu'utiliserait normalement tout navigateur Internet utilisé sur cet ordinateur à ce moment précis.

● (1545)

M. Alan Chapell: Je crois que c'est exact, monsieur, sauf que BlueKai n'utilise pas ces données. Nous offrons une plateforme qui permet à nos clients publicitaires d'utiliser ces données.

M. Blaine Calkins: Qui détient ces données?

M. Alan Chapell: Elles sont stockées par BlueKai.

M. Blaine Calkins: Elles sont stockées par BluKai, mais il y a aussi des données sur la machine locale. C'est dans les deux cas.

M. Alan Chapell: Oui, monsieur.

M. Blaine Calkins: Je peux créer une application. C'était mon métier avant, alors je peux créer une application qui, à son tour, créera un témoin et le stockera sur un ordinateur, et chaque fois qu'une personne entrera des renseignements dans un formulaire — prénom, nom, adresse etc. — ils seront stockés dans un témoin. La raison pour laquelle ils doivent être stockés dans un témoin est qu'une page Web est statique et non dynamique, même lorsque vous utilisez une page HTML dynamique, ou quelle qu'elle soit... Est-ce qu'il s'agit de termes que nous comprenons tous les deux?

M. Alan Chapell: Oui, monsieur.

M. Blaine Calkins: À titre informatif, si l'on utilise les témoins, c'est qu'ils sont des outils nécessaires. Il ne s'agit pas d'une application client-serveur. C'est une page statique, qui fait une transaction avec les autres serveurs qui se trouvent sur Internet à ce moment-là, quels qu'ils soient. Le témoin n'est là que pour stocker des renseignements. C'est un outil, parfois temporaire et parfois permanent, pour conserver les profils, les renseignements sur les usagers ou quoi que ce soit.

Voilà pourquoi lorsque nous retournons sur un certain nombre de sites Web différents, l'information selon laquelle nous y étions la dernière fois est déjà chargée automatiquement sur cette page Web. De cette façon, nous n'avons pas constamment à le faire. On nous demande de temps à autres si nous voulons qu'Internet Explorer sauvegarde les renseignements pour utilisation ultérieure. Ces renseignements sont stockés dans un témoin. Je comprends cela.

Voilà ce que j'ai besoin de savoir de votre point de vue: vous avez une option de refus, qui s'en remet à un témoin pour faire le suivi du signal ou autre qui indique que qu'ils ont refusé, mais comme mon collègue M. Angus l'a signalé, s'il choisit de désactiver les témoins et de supprimer la cache ou l'historique, et tous les témoins sont effacés, les renseignements concernant ce refus ne sont pas consignés dans l'ordinateur.

Est-ce exact?

M. Alan Chapell: Lorsque l'outil de refus ne se trouve pas dans le navigateur de l'utilisateur, alors la réponse à cette question est oui. Nous avons vu que c'était un problème sur le marché et c'est l'une des raisons pour lesquelles nous avons créé l'option de refus sur BlueKai. C'est un module externe de navigation.

M. Blaine Calkins: C'est un module externe.

M. Alan Chapell: Même lorsque les utilisateurs suppriment leurs témoins, le témoin de l'option de refus ne sera pas supprimé.

M. Blaine Calkins: Est-ce un module externe Java? Sinon, de quel type de module externe s'agit-il?

M. Alan Chapell: Je crois qu'il s'agit d'un module externe de navigation Java.

M. Blaine Calkins: C'est un module externe Java. D'accord.

Vous avez dit que vous aviez rendu le code source public.

M. Alan Chapell: En effet. Nous avons pris un code source...

M. Blaine Calkins: Alors n'importe qui...

M. Alan Chapell: ... fourni par Google...

M. Blaine Calkins: ... n'importe qui pourrait en faire l'ingénierie inverse. N'importe qui pourrait y jeter un coup d'oeil et quiconque a l'expérience voulue pourrait regarder le code et comprendre la nature de ce qui se passe. C'est un mécanisme de transparence pour BlueKai, c'est bien cela?

M. Alan Chapell: Eh bien...

M. Blaine Calkins: Il crée une plateforme standard que tout le monde peut utiliser et à laquelle tout le monde peut avoir accès.

M. Alan Chapell: C'est exact.

M. Blaine Calkins: C'est bien.

Pour en revenir à la question de la protection de la vie privée, qu'est-ce que vous offrez qui vous démarque des autres? Il me semble que vous n'offrez rien qui soit bien différent de ce qui se trouve déjà sur le marché pour n'importe quel agrégateur de données, sauf que vous avez ce registre, cette transparence accrue, qui permet aux gens de voir ce qu'il y a. En quoi cela est-il nouveau ou différent? Qu'est-ce que vous faites qui place la barre bien au-dessus de tout ce qui se fait sur le marché?

M. Alan Chapell: Si je ne m'abuse, il y a moins d'une dizaine de registres sur le marché en ce moment.

M. Blaine Calkins: Non, je...

M. Alan Chapell: Il pourrait y en avoir plus. Google en a un. Yahoo aussi. Je crois qu'il en va de même pour Microsoft. Il pourrait y avoir trois ou quatre autres entreprises qui en ont un. BlueKai en a un. Ce niveau de transparence n'est pas quelque chose que je qualifierais de commun sur le marché.

M. Blaine Calkins: Est-ce que c'est la capacité de l'utilisateur d'entrer directement dans ce registre qui vous démarque des autres?

M. Alan Chapell: Nous croyons que c'est un exemple d'innovation s'agissant de la protection de la vie privée.

M. Blaine Calkins: Je ne m'en prends pas à votre organisation. J'en comprends la valeur. La liberté aussi. Les gens veulent être libres de faire ce qu'ils veulent sur Internet et avoir leur mot à dire, mais ils se préoccupent aussi de leur vie privée.

Pouvez-vous éclairer le comité sur les capacités techniques qui permettraient aux utilisateurs de visiter un site Web qu'ils ne pourraient pas visiter s'ils choisissaient de désactiver leurs témoins ou de ne pas accepter de contrat de licence d'utilisateur?

Certaines personnes qui ont témoigné devant le comité nous ont dit à quel point il serait difficile d'offrir une plateforme qui tienne compte des préférences des utilisateurs en fonction du niveau de sécurité et du niveau d'interaction avec l'entreprise. Je ne crois pas que ce serait si difficile que cela à réaliser.

Pensez-vous que ce serait très difficile à faire? Par exemple, au lieu d'un système par lequel l'on accepte toutes les conditions d'un contrat de licence d'utilisateur en cliquant sur un seul bouton, l'industrie pourrait-elle faire en sorte qu'un visiteur n'accepte que certaines parties de ce contrat et puisse quand même visiter un site Web?

● (1550)

M. Alan Chapell: Eh bien...

M. Blaine Calkins: C'est une question difficile.

M. Alan Chapell: C'est une question très difficile. Nous n'avons pas de contrat de licence d'utilisateur.

M. Blaine Calkins: Je comprends.

M. Alan Chapell: À part BlueKai.com, nous ne sommes propriétaires ni gestionnaires d'aucun autre site Web. Il serait très utile d'avoir une plus grande granularité dans les déclarations de confidentialité parce qu'elle serait dans les contrats de licence d'utilisateur.

L'avis de confidentialité complexe que Martin Abrams chez Hunton & Williams et un certain nombre d'autres ont proposé au fil des ans est une avancée positive, mais il y a un hic: si vous placez un résumé au-dessus de vos pratiques relatives à la protection des renseignements personnels et votre jargon juridique tout en bas, un organe de réglementation pourrait penser que le résumé n'est pas en harmonie avec le jargon juridique. Au moins aux États-Unis, cela pourrait soulever un problème au plan de la réglementation. C'est l'un des points qui posent problème aux entreprises.

[*Français*]

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

[*Traduction*]

M. Blaine Calkins: Êtes-vous certain? Nous avons une conversation très intéressante.

Merci beaucoup.

[*Français*]

Le président: Je vais maintenant céder la parole à M. Andrews.

[*Traduction*]

M. Scott Andrews (Avalon, Lib.): Merci.

Bienvenue.

Peut-être que vous pourriez simplement m'expliquer votre plateforme et en quoi elle est anonyme. Vous avez des renseignements concernant une personne, mais ils sont toujours anonymes, et les annonceurs sont intéressés à obtenir ces renseignements anonymes. Expliquez-le-moi. Je ne saisis pas bien en quoi consiste votre modèle.

M. Alan Chapell: C'est un modèle pseudonyme dans lequel nous savons qu'un profil donné correspond à un navigateur en particulier. Ce navigateur peut être utilisé par une seule personne ou plusieurs. L'ordinateur peut avoir de multiples utilisateurs. Si vous visitiez, par exemple, un site de voyage, BlueKai ou une autre entreprise pourrait placer un témoin dans votre ordinateur. Ce témoin ne dit pas, par exemple, Alan Chapell. Il dit seulement « intéressé à aller à Hawaï ». Impossible d'identifier l'utilisateur à partir de la mention « voyage à Hawaï ».

J'imagine que des bien gens ici présents aimeraient bien aller à Hawaï en ce moment.

M. Scott Andrews: Les annonceurs sont attirés par ce modèle parce que..?

M. Alan Chapell: À certains égards, cela nous ramène aux principes de base du marketing direct. S'il est plus probable qu'une publicité particulière intéresse davantage un navigateur en particulier, l'annonceur est plus disposé à payer un gestionnaire de site Web pour qu'il place sa publicité. De cette façon, la publicité ciblée finance une bonne partie du contenu que les consommateurs consultent gratuitement.

M. Scott Andrews: Vous fournissez ces renseignements concernant le navigateur à l'entreprise qui veut faire de la publicité. C'est bien cela?

M. Alan Chapell: Nous fournissons une plateforme qui permet aux annonceurs qui font de la publicité en ligne de stocker des données et d'ensuite les analyser et les utiliser pour rehausser les renseignements concernant les futurs achats des médias numériques.

M. Scott Andrews: Y a-t-il une façon de relier les données que vous avez avec une personne hors ligne? Est-ce possible? Si l'annonceur obtenait les données et qu'il les obtenait d'une autre source avec le nom de la personne, serait-il possible de faire un lien entre les deux?

M. Alan Chapell: Dans ces types de discussions, vous voulez distinguer ce qui est théoriquement possible en laboratoire dans certains cas de ce qui est faisable du point de vue des affaires. Il suffit de retourner quelques années en arrière du côté, je pense, d'America Online, qui a communiqué par mégarde des données concernant les recherches en ligne. C'était un dossier si volumineux qu'un reporter a été en mesure d'identifier un certain nombre de personnes d'une liste qui comptait, je crois, des millions de noms. Cela a demandé beaucoup de travail. Depuis, je pense que l'industrie a pris des mesures supplémentaires pour faire en sorte qu'il soit encore plus difficile d'identifier une personne en particulier. Dans la technologie, je suppose qu'on ne peut jamais dire que c'est impossible, mais dans le cas de BlueKai, compte tenu de la façon dont nos systèmes de données sont configurés, je pense que nous y arrivons presque.

● (1555)

M. Scott Andrews: Merci.

[*Français*]

Le président: Je cède maintenant la parole à M. Carmichael.

[*Traduction*]

M. John Carmichael (Don Valley-Ouest, PCC): Merci, monsieur le président.

Merci, monsieur Chapell, d'être venu aujourd'hui. Mon collègue me donne une formation rapide.

Comme vous le savez, cette étude dure depuis un certain temps. Nous essayons de bien comprendre notre rôle de législateurs pour faire en sorte que l'on accorde la plus haute importance aux renseignements personnels des consommateurs. Dans le cadre de cette étude, nous avons abordé un certain nombre de domaines très préoccupants, et d'autres pour lesquels on nous a dit qu'il était préférable de ne pas contrecarrer l'industrie, car en leur imposant de la réglementation supplémentaire, on ne ferait qu'étouffer la croissance et l'emploi. Nous essayons de trouver un juste équilibre entre notre place dans ce processus et le besoin d'accorder une importance primordiale à la protection de la vie privée des consommateurs.

Comme vous le savez, nous avons surtout rencontré des représentants d'entreprises de médias sociaux. Je me demande si vous êtes d'accord pour dire que ces types d'entreprises pousseront le bouchon jusqu'à ce qu'on leur dise « ça suffit » par voie réglementaire. Diriez-vous que c'est une affirmation juste ou est-ce que j'exagère?

M. Alan Chapell: Je crois que l'on peut dire que les entreprises de médias sociaux contribuent à une culture de la protection de la vie privée en évolution. Par exemple, je m'intéresse aux question de protection de la vie privée depuis près d'une décennie. Dans cette optique, la notion de donner à un site Web une liste de tous vos contacts et les activités auxquelles vous participez et les photos de vos amis aurait été impensable il y a 10 ans, mais aujourd'hui, c'est relativement courant. Facebook a même un peu soulevé la controverse en offrant le premier flux de nouvelles, et un certain nombre de personnes ont hurlé qu'il s'agissait d'une atteinte à la vie privée.

Tant d'un point de vue législatif que réglementaire, il est difficile de définir l'équilibre qu'il faut trouver entre étouffer l'innovation et protéger la vie privée des consommateurs. Fort heureusement, au Canada, même si je ne prétends pas être un spécialiste du droit relatif au respect de la vie privée, je sais qu'un cadre assez exhaustif est déjà en place et qu'un programme d'autoréglementation sera lancé au cours des prochains mois.

De mon point de vue, il serait bon de voir comment ce programme évolue avant de prendre des mesures proactives. Il faudrait au moins donner à l'industrie l'occasion de montrer que c'est dans l'intérêt du consommateur.

M. John Carmichael: J'espère avoir suffisamment de temps pour y revenir avant de terminer, mais je suis certain que certains de mes collègues poursuivront dans la même veine.

Quand vous parlez des données de préférences et des contraintes liées à la protection des renseignements personnels qui entourent BlueKai, lorsque les données tombent dans votre coffre-fort de données — faute de terme plus approprié — et que les consommateurs déterminent qu'ils ne veulent pas que leurs renseignements soient diffusés pour une raison ou une autre, quand ils activent l'option de refus sur ce témoin, j'ai lu quelque part qu'il faut compter six mois, je crois, avant que les données soient supprimées. Je ne sais pas si c'est exact; vous pouvez me corriger.

Lorsque j'ai choisi l'option de refus avec mes données — il s'agit des renseignements stockés chez BlueKai ou chez tout autre agrégateur — ai-je raison de penser que les données sont entièrement supprimées?

M. Alan Chapell: Elles le sont. Je pense que lorsque vous dites six mois, vous parlez de la période de rétention des données de BlueKai, mais cela n'a rien à voir avec la période de retrait.

Une fois qu'un utilisateur a choisi l'option de retrait et que BlueKai a affiché un témoin de retrait, il remplace effectivement les autres témoins de BlueKai et annule ce dossier en particulier.

● (1600)

M. John Carmichael: Alors l'historique que j'accumule dans BlueKai pendant la période où nous avons été amis est entièrement supprimé?

M. Alan Chapell: Je crois qu'on peut dire que le témoin de retrait enlève toutes les données ciblées et les données de préférences qui se trouvent sur cet ordinateur, si bien qu'elles ne peuvent plus servir au ciblage publicitaire.

M. John Carmichael: Sommes-nous revenus à la question de l'anonymat maintenant et à la rétention des données de préférences des annonceurs, etc.?

M. Alan Chapell: Je pense que dans la mesure où les données sont stockées pendant un certain temps par, disons, un annonceur qui place des publicités en format numérique, les données pseudonymes seront préservées au fil du temps. L'option de retrait est typiquement axée sur l'avenir, et ils en viendront à ne plus faire de publicité comportementale en ligne.

Je pense qu'il devient très difficile de détruire toutes les données rétroactivement. Il y a des gens qui sont beaucoup plus éloquents que je le suis, mais j'encouragerais le comité à prendre connaissance de certaines des discussions que l'on tient à l'Union européenne concernant le droit d'être oublié.

M. John Carmichael: D'accord.

Combien de temps me reste-t-il, monsieur le président?

Le président: Il vous reste 45 secondes.

M. John Carmichael: Comme nous allons bientôt terminer notre étude, quelles questions nous recommanderiez-vous d'examiner ou d'envisager pour rehausser l'efficacité de la protection des consommateurs — les consommateurs canadiens en particulier — pour ce qui est de la façon dont leurs renseignements personnels sont utilisés?

M. Alan Chapell: Je pense qu'une bonne façon de commencer serait de permettre au programme d'autoréglementation de se développer. Ensuite, je suggérerais une interaction régulière, que cela vise strictement le Commissariat à la protection de la vie privée, le ou les deux, mais je pense qu'une vérification régulière — je ne veux pas parler de bulletin — pourrait être une bonne façon pour le comité de continuer à superviser l'élaboration du programme d'autoréglementation.

Ces choses n'arrivent pas habituellement du jour au lendemain. J'en ai fait l'expérience aux États-Unis, mais je pense que...

M. John Carmichael: Nous allons dans la bonne direction?

M. Alan Chapell: Nous allons dans la bonne direction.

M. John Carmichael: Merci beaucoup.

[*Français*]

Le président: Merci, monsieur Carmichael.

Je cède maintenant la parole à Mme Borg pour cinq minutes.

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

Cette discussion est fort intéressante, et je remercie nos témoins d'être présents parmi nous aujourd'hui.

Ma première question concerne les clients qui utilisent votre programme et vos services.

Comment un utilisateur d'Internet peut-il déterminer qu'une entreprise donnée a recours à vos services, de façon à pouvoir ensuite se rendre sur votre site Web et indiquer qu'il ne veut plus être assujetti à certaines dispositions? Est-ce que c'est indiqué quelque part? Est-ce accessible aux utilisateurs d'Internet?

[*Traduction*]

M. Alan Chapell: Nous voyons de plus en plus d'utilisateurs d'Internet télécharger leurs propres outils pour assurer la transparence. Je pense notamment à Ghostery, mais je crois qu'il y en a d'autres. Il s'agit de modules externes axés sur les navigateurs qui indiquent aux utilisateurs d'Internet quels témoins sont communiqués par quelles entreprises sur les sites Web qu'ils visitent. Il est clair que l'on peut fournir aux utilisateurs ce mécanisme assorti d'une transparence accrue. Nous voyons de plus en plus d'utilisateurs d'Internet employer exactement ces types d'outils.

De plus, dans le programme d'autoréglementation de l'industrie — et je parle ici des États-Unis — il y a deux sites Web. Il y en a un qui s'appelle networkadvertising.org et l'autre, aboutads.info. Ils permettent tous les deux aux utilisateurs de ne pas recevoir de publicité de toutes les entreprises membres.

Encore une fois aux États-Unis, il est probablement utile de rappeler que nous voyons de plus en plus de petites icônes axées sur l'avenir dans les publicités numériques qui sont ciblées grâce aux données de publicité comportementale en ligne. Il est possible que l'utilisateur ne sache pas quelle entreprise le cible simplement en regardant le petit point sur la publicité, mais c'est un mécanisme qui lui permet de comprendre un peu mieux la pratique de la publicité comportementale en ligne et d'ensuite aller à la page où il peut se prévaloir de son option de retrait.

● (1605)

[*Français*]

Mme Charmaine Borg: Merci.

Donc, si je comprends bien, c'est l'utilisateur qui doit recourir à ces outils pour savoir ce qu'il en est.

Ma prochaine question concerne encore une fois vos clients.

Lorsque vous vendez vos produits ou que vous entrez en contact avec un client, encouragez-vous la protection des renseignements personnels?

[*Traduction*]

M. Alan Chapell: Oui, nous le faisons.

Je me trouve engagé dans beaucoup d'interactions avec les clients, voire la plupart, pour informer ces entreprises des règles en matière de protection de la vie privée. Une partie de cela dépend de l'administration et une autre, du type de données utilisées, mais nous prenons la chose très au sérieux. Nous estimons que l'un de nos rôles sur le marché est d'informer les clients des règles de conduite en matière de protection de la vie privée.

[*Français*]

Mme Charmaine Borg: Durant votre présentation et en réponse à ma question, vous avez parlé des principes à suivre.

Pourriez-vous nous donner plus de détails sur les principes que vous encouragez, en tant que membre des associations que vous avez mentionnées, ainsi que comme compagnie utilisatrice de ces données?

[*Traduction*]

M. Alan Chapell: Bien sûr.

Je vais parler surtout des États-Unis. Il est clair que nombre de ces concepts fonctionnent dans d'autres administrations.

La première organisation que j'ai mentionnée est la Network Advertising Initiative. Il s'agit d'une association commerciale de l'industrie qui existe depuis une douzaine d'années. Elle se compose principalement de ce que nous appelons les intermédiaires Internet: les réseaux, les plateformes, les échanges et les agrégateurs de données. Ces organes se trouvent entre les diffuseurs de sites Web et les annonceurs. Ils facilitent ce processus.

Avec ces entreprises, ce qu'il y a toujours eu de difficile est que, puisqu'elles ne contrôlent ni la publicité ni le site Web, elles ne peuvent pas aisément diffuser les normes en matière de protection de la vie privée dans le reste de l'écosystème. Ces normes supposent des avis, de la transparence, une option de retrait et une règle en ce qui touche ce que nous appelons les « données sensibles ».

Lorsque je fais référence à la Digital Advertising Alliance, je fais allusion à ce qui représente plutôt une vaste coalition d'associations de l'industrie, dont la Network Advertising Initiative. Cela dit, elle englobe aussi les diffuseurs en ligne et les agences de publicité numérique.

La Digital Advertising Alliance a pour mandat de veiller à ce que toutes les normes en matière de protection de la vie privée soient harmonisées dans l'écosystème d'une entreprise.

[*Français*]

Le président: Merci, madame Borg. Votre temps de parole est écoulé.

Je laisse maintenant la parole à M. Butt, pour cinq minutes.

[*Traduction*]

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

Merci, monsieur Chapell, d'être venu témoigner devant le comité.

Diriez-vous que vous connaissez bien le mandat actuel de la Commissaire à la protection de la vie privée au Canada, ses rôles et responsabilités et son interaction générale avec le milieu des affaires — probablement avec nombre de vos clients — , etc.? Diriez-vous que vous connaissez bien son rôle actuel?

M. Alan Chapell: Je crois le connaître relativement bien.

M. Brad Butt: Compte tenu de ce fait et de certaines des questions que notre comité étudie — son rôle et l'interaction — je me préoccupe notamment du fait que, malgré les meilleures intentions, il arrive au gouvernement de réglementer à outrance ou de fixer des paramètres qui étouffent en fait l'innovation et la créativité.

Ce qui m'inquiète surtout avec les médias sociaux et autres est que la technologie évolue si rapidement. Je ne suis pas toujours entièrement sûr que le gouvernement soit capable de suivre l'évolution rapide des médias sociaux et des secteurs connexes.

Si j'en juge par votre témoignage, il semble que vous diriez que votre organisation fonctionne plutôt dans un milieu d'autoréglementation, que vous essayez de faire du mieux que vous pouvez comme entreprise pour respecter les questions de protection de la vie privée, et que vous fonctionnez dans un milieu approprié, etc.

Est-ce un modèle suffisamment fort, à votre avis, pour veiller à ce que nous nous efforcions tous dans la mesure du possible de protéger la vie privée des gens tout en faisant en sorte que les personnes qui arrivent à suivre les avancées technologiques puissent réagir beaucoup plus vite que nous, députés, pouvons le faire en essayant d'adopter des lois et de donner suite à des choses qui se sont déjà produites? Avez-vous d'autres conseils à nous donner à cet égard?

● (1610)

M. Alan Chapell: Je suis d'accord avec tout ce que vous avez dit.

J'ajouterais que le défi, lorsque l'on rédige des lois dans un environnement technologique en rapide évolution, est la proverbiale loi des conséquences imprévues. On estime généralement que le gouvernement n'a pas intérêt à choisir des gagnants et des perdants dans un média en émergence ou, en fait, dans tout marché. Ce qu'il y a de difficile avec n'importe quel type de loi est que, presque par définition, quand elle finit par être adoptée, elle est désuète.

Ce qu'il y a de bien avec l'autoréglementation, si elle est assortie d'un mécanisme d'application adéquat, est qu'elle peut continuer à s'adapter à l'innovation sur le marché.

M. Brad Butt: Le Commissariat à la protection de la privée au Canada a-t-il eu une interaction ou un engagement directs avec Bluekai, soit en prenant contact avec vous et en disant qu'un point le préoccupait ou qu'il avait entendu dire quelque chose ou que quelqu'un s'était plaint auprès de lui de votre organisation? Avez-vous eu ce genre d'interaction avec notre Commissaire à la protection de la vie privée?

M. Alan Chapell: Pas directement, non.

Je crois qu'il y a eu de l'interaction il y a environ deux ans et demi. Je préside le comité sur la protection de la vie privée d'un groupe qui s'appelle Mobile Marketing Association. Nous élaborions des normes il y a deux ou trois ans, et je crois qu'il y avait de l'interaction. Ce n'était pas une interaction dirigée de ma part. C'est simplement pour que vous sachiez qu'il y avait au moins un peu d'interaction, mais nous n'avons pas reçu de plainte.

M. Brad Butt: Est-ce que c'était plutôt pour obtenir des conseils ou était-ce que le commissariat vous donnait des renseignements? Demandiez-vous conseil au commissariat pour rédiger des lignes directrices que l'industrie elle-même pourrait envisager de suivre? Était-ce plutôt une ressource pour votre organisation? Était-ce son principal rôle à l'époque?

M. Alan Chapell: Oui, ce l'était. Je pense que le commissariat a eu l'amabilité de prodiguer des conseils à la Mobile Marketing Association.

M. Brad Butt: Avez-vous trouvé que ce rôle du commissariat était utile? Cela vous a-t-il aidé à rédiger des lignes directrices? Pour en revenir au régime d'autoréglementation, la Commissaire à la protection de la vie privée et son personnel ont-ils été en mesure de vous donner des conseils utiles pour vous aider à façonner le modèle que vous utilisez?

M. Alan Chapell: Tout à fait.

Pour être bien clair, par contre, je n'ai pas fait d'intervention directe; il y avait des gens dans l'équipe. Ce que je veux dire c'est que dans tout processus auquel participent de multiples intervenants, il y aura un certain nombre de groupes qui interagissent. Je crois que les interactions étaient très valables.

M. Brad Butt: C'est ma dernière question, monsieur le président, avant de céder la parole à quelqu'un d'autre.

Elle se rapporte à un voyage que certains membres du comité ont effectué à Washington. Nous avons rencontré les représentants d'excellentes organisations, dont la FTC et d'autres.

De votre point de vue, y a-t-il quelque chose que l'on fait bien aux États-Unis et dont nous pourrions tirer des leçons? Avez-vous des conseils à formuler en fonction de votre interaction comme entreprise américaine et non canadienne qui pourrait nous être particulièrement utile? Les représentants d'organisation que nous avons rencontrés ont-ils dit vrai en affirmant que le Canada était pas mal en avance sur les États-Unis à bien des égards dans ce domaine?

M. Alan Chapell: Je crois que je suis d'accord avec la dernière proposition. À certains égards, je pense que nous pourrions tirer des leçons de l'expérience canadienne.

Dans les discussions concernant l'autoréglementation de la publicité comportementale en ligne, je crois comprendre — encore une fois, je n'y ai pas participé directement, mais j'ai parlé à un certain nombre de personnes qui l'ont fait — que les discussions étaient beaucoup moins litigieuses. Toutes les parties ont reconnu qu'il était nécessaire de faire un compromis.

J'estime vraiment que le résultat net sera un programme qui trouve le juste équilibre. Il nous est arrivé de ne pas atteindre ce but aux États-Unis.

[*Français*]

Le président: Merci, monsieur Butt.

Au nom du comité, je vous remercie, monsieur Chapell, d'avoir bien voulu venir nous rencontrer pour nous aider dans notre étude.

Nous allons suspendre la séance pendant quelques minutes. Nous entendrons par la suite la commissaire à la protection de la vie privée.

Merci encore.

● (1615)

[*Traduction*]

M. Alan Chapell: Merci, monsieur, et merci au comité. Ce fut un honneur.

[*Français*]

Le président: Nous allons reprendre nos travaux.

Je remercie la commissaire Mme Stoddart de sa présence parmi nous ainsi que les deux personnes qui l'accompagnent, soit Mme Bucknell et Mme Bernier. Cela fait déjà un certain temps que nous faisons cette étude et nous avons entendu de bons mots à votre sujet. Je voulais vous le mentionner avant que vous commenciez.

Vous aurez une période de dix minutes pour faire votre présentation. Par la suite, comme d'habitude, il y aura une période questions. Les membres du comité auront sans doute des questions pour vous. Sans plus tarder, je vous laisse la parole.

Mme Jennifer Stoddart (commissaire à la protection de la vie privée du Canada, Commissariat à la protection de la vie privée du Canada): Merci beaucoup, monsieur le président, de votre invitation à comparaître à nouveau à la toute fin de votre étude que nous avons suivie avec intérêt.

[*Traduction*]

Je suis accompagnée par Chantal Bernier, commissaire adjointe à la protection de la vie privée, qui s'occupe de nos activités courantes, et par Barbara Bucknell, analyste des politiques stratégiques, qui est spécialiste des médias sociaux. J'espère qu'elles m'aideront à répondre à vos questions.

Mesdames et messieurs, j'aimerais commencer par vous donner un aperçu des enjeux en matière de protection de la vie privée.

Au cours des derniers mois, je crois que vous avez entendu un éventail de parties intéressées s'exprimer sur les avantages et les défis pour la protection de la vie privée associés aux médias sociaux. Lorsque j'ai comparu devant vous pour la première fois en mai, j'ai énuméré les quatre aspects qui nous préoccupaient le plus sur le plan de la protection de la vie privée. Ces aspects étaient les suivants: la responsabilité, le consentement valable, la limitation de l'utilisation et la conservation. Il convient de noter que les témoins qui se sont présentés devant vous étaient largement d'accord pour dire que ces enjeux sont mis au défi par les médias sociaux. Toutefois, je crois comprendre qu'ils ne semblaient pas toujours s'accorder sur la pertinence des solutions offertes pour aborder les problèmes.

Il convient également de noter que la protection de la vie privée des jeunes et des enfants a été omniprésente dans la discussion. De nombreuses idées intéressantes ont été proposées relativement à la culture numérique ainsi qu'aux réponses législatives possibles.

Monsieur le président, j'aimerais féliciter le comité d'avoir eu la clairvoyance de mener une étude aussi pertinente.

J'aimerais aujourd'hui me pencher sur les principales observations découlant des témoignages que vous avez entendus.

La plus importante question mise de l'avant tout au long de l'étude concernait la capacité de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) de relever les défis liés à l'évolution de la technologie. La plupart des témoins étaient d'avis que la LPRPDE avait besoin d'être modernisée, tandis que d'autres estimaient que la LPRPDE n'avait pas besoin d'être modifiée, que son modèle d'application de la loi fonctionnait et que sa force résidait dans sa neutralité par rapport à la technologie.

Selon moi, l'émergence de géants Internet menace l'équilibre recherché par l'esprit et la lettre de la LPRPDE. Le quasi-monopole exercé par ces multinationales a rendu inefficace, selon moi, l'approche toute en douceur de LPRPDE, qui repose sur des recommandations non contraignantes et sur une menace de ternir la réputation. Nous avons vu des organisations ignorer nos recommandations jusqu'à ce que la Cour soit saisie de l'affaire, et nous avons vu de grandes entreprises, au nom d'une consultation avec le commissariat, s'engager à mettre en place des mesures répondant à nos préoccupations pour ensuite ignorer nos conseils. Par ailleurs, compte tenu des vastes quantités de renseignements personnels détenus par les organisations sur des plateformes de plus en plus complexes, le risque lié à des atteintes importantes et à des utilisations inattendues, non souhaitées, voire même envahissantes, de ces renseignements exige la mise en place de mesures de sécurité et de conséquences financières adaptées qui ne sont pas actuellement prévues par la LPRPDE.

De nouvelles mesures incitatives, y compris l'apport de changements au modèle d'application de la loi, sont requises pour inciter les organisations à se montrer proactives, à mettre en place des protections qui s'appliquent dès le départ et à veiller au traitement sécuritaire des renseignements personnels des gens. Je suis d'accord avec les témoins qui ont déclaré que la force de LPRPDE est qu'elle est neutre sur le plan technologique et qu'elle est fondée sur des principes. Nous croyons que ces caractéristiques doivent demeurer.

● (1620)

[*Français*]

Je suis également d'accord, du moins en partie, avec ceux qui ont souligné le succès du commissariat à amener les organisations à respecter davantage la loi. Nous avons utilisé les outils que fournit la loi et nous avons été en mesure de procéder à certains changements, souvent après des efforts ardus. Ces efforts ont coûté cher à la population canadienne et ils sont de moins en moins efficaces contre les puissances multinationales.

On vous a dit que le commissariat ne peut être — et je reprends des mots qui ont été prononcés très souvent dans vos délibérations — le juge, le jury et le bourreau. En réponse à cet argument, j'aimerais attirer votre attention sur la situation de certains de mes homologues internationaux et même provinciaux.

Le commissaire du Royaume-Uni peut imposer des amendes, tout comme peuvent le faire bon nombre des autorités internationales de protection des données qui figurent dans le document que j'ai présenté aujourd'hui. Au Royaume-Uni, mes homologues détiennent plus de pouvoirs en matière d'application de la loi, ce qui n'a pas empêché la mise en place d'une approche de l'ombudsman. Des amendes sont en effet imposées lorsqu'une méthode plus indulgente n'a pas fonctionné. Nos homologues nous disent que les entreprises qui s'engagent dès le départ à adopter de bonnes pratiques pour la protection de la vie privée croient qu'imposer un fardeau financier à celles qui ne le font pas rend la concurrence plus équitable.

Les commissaires du Québec, de l'Alberta et de la Colombie-Britannique ont le pouvoir de délivrer des ordonnances et de régir le secteur privé. Ils ont également d'autres fonctions, prescrites par la loi, qui leur permettent de jouer de nombreux rôles, soit celui d'éducateur, d'arbitre, d'exécuteur, de défenseurs, etc. J'ai remarqué que les témoins ayant pris la parole devant le présent comité n'avaient que de bons commentaires à faire sur les relations qu'ils avaient eues avec eux. Des témoins ont dit que le modèle canadien faisait l'envie de nombreux pays partout dans le monde.

Ce qu'ils aiment à propos de la loi, c'est qu'elle n'exclut pas de secteurs et qu'elle est non normative. Pourtant, un grand nombre de mes homologues étrangers ont des outils plus puissants en matière d'application de la loi, ou ils en font la demande. C'est donc dire que ce n'est pas notre modèle d'application de la loi qu'ils admirent.

En fait, je suis inquiète de ceci. Si mes homologues continuent d'obtenir plus de pouvoirs, mais que le Canada ne bouge pas, nous prendrons du retard et les consommateurs cesseront d'avoir confiance. Or cette confiance est nécessaire pour que l'économie numérique prospère.

Nous pourrions au moins commencer par établir un avis obligatoire d'atteinte à la protection des données, y compris des conséquences financières dans les cas flagrants. De plus en plus de pays adoptent des lois semblables. Ces mesures renforceraient la responsabilité. De plus, des sanctions, sur le plan financier, inciteraient à une meilleure protection des renseignements personnels de la population canadienne. Ces sanctions seraient souples et devraient s'adapter à la situation afin de ne pas imposer un fardeau excessif aux petites organisations.

● (1625)

[*Traduction*]

J'aimerais maintenant parler un peu de culture numérique.

L'importance de la culture numérique est un autre sujet clé dont il a été question pendant les audiences. Je crois que le temps est également venu pour les gouvernements, les éducateurs et les collectivités de se concentrer sérieusement sur l'éducation numérique des Canadiennes et Canadiens de tous âges.

Il est impératif de s'intéresser aux questions éthiques et sociales plus vastes qui sont soulevées par les nouvelles technologies de l'information, mais qui ne relèvent pas à proprement parler de lois en matière de protection des données. Les gens doivent comprendre que les renseignements publiés sur Internet peuvent s'y retrouver pour l'éternité et qu'il faut faire très attention à ce que l'on publie à propos de nous et des autres. Cela étant dit, la culture numérique ne dispense pas les entreprises de leurs responsabilités en vertu des lois en matière de protection de la vie privée.

En conclusion, monsieur le président, vu la nature mondiale de l'économie numérique d'aujourd'hui, la loi fédérale du Canada doit être dotée de pouvoirs comparables à ceux des autres gouvernements afin d'avoir le plus grand impact sur la protection de la vie privée et de renforcer la confiance qu'accorde la population canadienne à l'environnement en ligne.

Une loi qui a été créée à une époque où les réseaux sociaux, les téléphones mobiles et les technologies intelligentes n'existaient pas encore ne peut rester inchangée. Les moyens par lesquels les renseignements personnels peuvent être recueillis et utilisés dans cet environnement par de nombreux acteurs font en sorte qu'il devient de plus en plus urgent de mener une étude officielle à propos de l'efficacité de notre cadre de protection de la vie privée. J'encourage fortement le gouvernement à procéder le plus rapidement possible à un examen de la loi, notamment de la LPRPDE.

Merci infiniment encore une fois de m'avoir invitée. Mes collègues et moi-même nous ferons un plaisir d'essayer de répondre à vos questions.

Merci.

[*Français*]

Le président: Merci beaucoup.

Madame Borg, vous disposez de sept minutes.

Mme Charmaine Borg: Merci beaucoup, monsieur le président.

Merci, madame Stoddart, d'être parmi nous aujourd'hui.

Après avoir entendu tous ces témoignages, c'est un plaisir d'entendre maintenant vos commentaires. Des opinions divergentes ont été exprimées. On nous a même fait part d'opinions à portée internationale. Ça nous a vraiment été utile.

Vous avez déclaré récemment dans les médias que les dispositions du projet de loi C-12 portant sur l'atteinte aux données ne protégeaient pas suffisamment les renseignements personnels des Canadiens. Vous avez même dit, dans ces circonstances, ne pas pouvoir appuyer à 100 % ce projet de loi.

Pourriez-vous nous dire comment celui-ci devrait être modifié pour protéger adéquatement les renseignements personnels des Canadiens?

Mme Jennifer Stoddart: Je vous remercie de la question.

J'ai rencontré officiellement le sous-ministre d'Industrie Canada ce printemps. Je lui ai dit que les choses avaient énormément changé depuis le moment où le projet de loi C-12 avait été présenté à la Chambre. Je pense que ça remonte à plus de deux ans. Nous en avions discuté, à l'époque. J'ai dit que d'autres pays avaient adopté une loi et que, dans sa forme actuelle, le projet de loi C-12 n'était pas une réponse adéquate à la menace continue et grandissante que constituent la fuite des données et les bris de confidentialité relatifs aux données. Nous pourrions au minimum considérer le seuil qui est décrit, mais plus important encore, il faudrait adopter un système de pénalités, voire d'amendes, qui inciterait à investir dans la protection des données et qui aurait un effet dissuasif à l'égard des bris de confidentialité.

Mme Charmaine Borg: Merci beaucoup.

Plusieurs témoins ont souligné le fait que vous n'aviez pas assez de pouvoirs. Vous l'avez souligné également lors de votre discours. Même lorsqu'on est allés aux États-Unis, les gens ont dit que la commissaire canadienne faisait un excellent travail, mais qu'elle avait besoin de pouvoirs supplémentaires pour bien remplir son mandat.

Il y a de nombreuse poursuites contre des compagnies comme Facebook existent parce que c'est le seul recours qui existe. Si on étendait vos pouvoirs pour que vous puissiez rendre des ordonnances et imposer des amendes, quel serait le meilleur modèle sur lequel on pourrait se baser? On a l'exemple de l'Alberta, du Québec et de l'Ontario. Un modèle est-il préférable à un autre? Y en a-t-il un qui fonctionne mieux selon vous?

● (1630)

Mme Jennifer Stoddart: Avant de conclure, je pense qu'il serait préférable que le comité se penche sur les différents modèles. Différentes options existent et il faut considérer les sanctions administrative, les amendes et la possibilité de se rapporter à la Cour fédérale pour demander des dommages statutaires.

Dans l'intérêt de la stabilité administrative, le modèle qui dérange le moins, et qui est donc préférable, est le statu quo. Encore une fois, je pense que le comité devrait se pencher sur cette question. Lorsque le besoin survient ou que cela est nécessaire, le commissariat pourrait demander à la Cour fédérale de rendre une ordonnance. Cela ne changerait pas fondamentalement tout le modèle de fonctionnement.

Mme Charmaine Borg: Merci.

Ma prochaine question porte sur la différence entre le consentement implicite et explicite. C'est un sujet qu'on a beaucoup abordé tout au long de cette étude.

Selon vous, est-il possible d'exiger que les entreprises ou les compagnies de réseaux sociaux utilisent un système où le consentement explicite est demandé partout? Est-ce possible sur le plan technique et est-ce souhaitable?

Mme Jennifer Stoddart: Je demanderais à Mme Bucknell de répondre.

Mme Charmaine Borg: D'accord.

Mme Jennifer Stoddart: Elle a passé des jours, voire des mois, à travailler sur cette question. Il me semble que cela dépend du type de questions ou du contexte dans lequel on demande le consentement. Dans certains cas, cela s'applique et dans d'autres, non.

Mme Bucknell a sûrement des observations à faire sur ce sujet.

[*Traduction*]

Mme Barbara Bucknell (analyste en politiques stratégiques, Direction des services juridiques, des politiques et des recherches, Commissariat à la protection de la vie privée du Canada): Merci.

Je crois que c'est possible, mais les organismes ont besoin de s'attacher à la meilleure façon de le faire, car cela présente clairement des défis. Il est certain que dans l'environnement mobile, l'espace et la taille sont limités, mais cela ne signifie pas qu'il soit impossible de dire aux gens très clairement et très simplement, par exemple, voilà les renseignements que nous allons communiquer si vous téléchargez cette application.

Nous avons travaillé d'arrache-pied à formuler des lignes directrices en matière de publicité comportementale en ligne ainsi que des lignes directrices en matière d'application mobile, que nous avons récemment publiées, pour renforcer le message que oui, cela peut être fait, et que cela devrait l'être en des termes clairs et simples. Je pense que notre commissariat en produira d'autres.

[*Français*]

Mme Charmaine Borg: Merci beaucoup.

Ma prochaine question concerne les politiques sur la protection de la vie privée et sur l'utilisation des données.

On a observé, tout comme vous, que les entreprises changeaient leurs politiques au fil du temps. Pensez-vous que les entreprises devraient être obligées de demander à nouveau le consentement de l'abonné ? Cette question a un lien avec celle du consentement explicite. Est-il possible pour ces entreprises d'informer les utilisateurs qu'elles ont changé leurs politiques et de demander s'ils veulent encore y adhérer?

Mme Jennifer Stoddart: Je crois que les entreprises devraient signaler à leurs abonnés, ou à leur clientèle, que les conditions ont changé, car le consentement que le consommateur a donné lors de son adhésion ne portait pas sur les nouvelles conditions. Il faudrait que la compagnie signale au moins que les règles du jeu ont changé pour que le consommateur ait alors le choix entre continuer et terminer son abonnement.

Le président: Merci, madame Borg. Malheureusement, votre temps est écoulé.

Je cède maintenant la parole à Mme Davidson pour sept minutes.

[*Traduction*]

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

Bienvenue, madame la commissaire. C'est un plaisir de vous revoir ainsi que les collègues qui vous accompagnent. Nous vous savons gré d'être venue.

L'étude a été longue, mais bonne, je pense. Nous avons entendu des commentaires très intéressants et nous avons écouté les témoignages de gens et de représentants d'entreprises très intéressants. Je crois que cela a été très utile et je me réjouis que nous ayons entrepris cette étude.

Comme vous l'avez indiqué dans vos remarques, certains « témoins étaient d'avis que la LPRPDE avait besoin d'être modernisée, tandis que d'autres estimaient que la LPRPDE n'avait pas besoin d'être modifiée, que son modèle d'application de la loi fonctionnait et que sa force résidait dans sa neutralité par rapport à la technologie ». Je lis simplement la transcription des commentaires que vous avez formulés tout à l'heure.

Nous avons entendu les témoignages de beaucoup de personnes concernant les deux côtés de cette question. Ils se sont dits préoccupés que l'on songe à accorder des pouvoirs accrus, notamment les pouvoirs d'exécution et la capacité d'imposer des sanctions, et que cela mine la bonne relation que votre commissariat entretient actuellement avec nombre d'entreprises que vous examinez.

Pouvez-vous répondre à cette préoccupation? Estimez-vous que cela influera sur votre capacité de bien gérer la relation avec ces entreprises? Si vous aviez des pouvoirs d'exécution accrus, en quoi cela influerait-il sur votre relation actuelle avec les entreprises privées? Vous avez affirmé tout à l'heure que certaines personnes vous disent que le commissariat ne peut être le juge, le jury et le bourreau. Comment cela fonctionnerait-il? Où serait le juste équilibre? Y aurait-il des contrôles? À votre avis, est-ce au commissariat d'en décider?

● (1635)

Mme Jennifer Stoddart: Merci, honorable député.

Je suis un peu étonnée par cette déclaration. On a l'impression que, si nous avions plus de pouvoir, nos discussions seraient très hargneuses. Je ne sais pas quelles seraient les conséquences si nous avions des pouvoirs de contrainte.

J'ai eu l'honneur de présider un tribunal dont j'ai parlé dans l'exposé qui applique la loi sur la protection des renseignements personnels au Québec, concernant les secteurs public et privé. Nos relations avec les entreprises privées n'étaient pas particulièrement acrimonieuses. Ce n'est pas ce que je constate non plus concernant mes collègues de la Colombie-Britannique et de l'Alberta, parce qu'ils font également de la sensibilisation. Nous préférons si possible négocier pour régler les différents. Personne ne veut aller en cour si d'autres solutions existent. Nous faisons la promotion du respect volontaire de la loi.

C'est pourquoi personne ne dit que les relations sont ardues dans les régions du Canada où il y a des pouvoirs de contrainte. En cas de poursuite, les gens s'entendent pour dire qu'il y a désaccord, mais ça n'empêche pas mes collègues ou moi de faire de la sensibilisation, de travailler avec les chefs de la protection des renseignements personnels et de tenir des réunions avec le secteur privé.

Je suis plutôt perplexe quant à cette déclaration.

Mme Patricia Davidson: Bien des témoins nous ont dit qu'ils avaient une excellente relation avec le commissariat; je pense que c'est la majorité. Ils ne veulent pas qu'elle soit mise en péril.

Pouvez-vous simplement en dire plus sur le juge, le jury et le bourreau? Ce ne sont pas des termes toujours très positifs, mais comment voyez-vous la question?

Mme Jennifer Stoddart: Ce commentaire me renverse aussi. Le concept de ce que nous appelons les organisations administratives multifonctionnelles est, en fait, très bien connu dans le droit canadien. Je crois qu'il en va de même avec le droit britannique et le droit australien, si on examine les lois d'intérêt public qui ressemblent le plus à la nôtre. Mes collègues de l'Australie et du Royaume-Uni ont différentes fonctions de sensibilisation de l'entreprise et de la population, d'arbitrage et de médiation. Le commissaire au Royaume-Uni peut imposer des amendes. Celui de l'Australie peut intenter une poursuite et exiger une amende de plus d'un million de dollars australiens. Ce modèle est très bien connu à l'échelle internationale.

Il est très bien connu au pays aussi. Je répète que mes collègues de la Colombie-Britannique et de l'Alberta font de la sensibilisation avec nous. Nous avons produit ensemble plusieurs documents d'orientation. Ces commissariats sensibilisent la population et rendent des jugements. Leurs conclusions sont contraignantes. Je ne sais pourquoi, tout d'un coup, nous n'aurions plus les mêmes pouvoirs qu'avant. Ces pouvoirs sont la norme en Alberta, en Colombie-Britannique, au Québec et à l'étranger depuis 15 ans.

● (1640)

Mme Patricia Davidson: Ces commissariats ont-ils un processus d'arbitrage?

Mme Jennifer Stoddart: Je ne suis pas sûre...

Mme Patricia Davidson: Je devrais plutôt parler d'un processus d'appel.

Mme Jennifer Stoddart: Oui, il y a un processus d'appel. Au Québec, on peut interjeter appel directement. Je crois qu'il y a un contrôle judiciaire en Alberta et en Colombie-Britannique, qui constitue en général une norme supérieure à mon avis.

Mme Patricia Davidson: Votre exposé portait aussi sur la culture numérique. Un éventail très large de témoins nous en ont parlé durant notre étude.

Il en a été question concernant les enfants, mais aussi à propos des adultes. Un certain groupe d'âge connaît assez bien les réseaux sociaux, mais un autre n'y est pas du tout sensibilisé. Pour leur part, les jeunes apprennent en très bas âge.

Que faut-il faire selon vous en ce qui a trait à la culture numérique? Qui doit s'en charger? S'agit-il d'une responsabilité partagée? Votre commissariat va-t-il s'impliquer davantage à cet égard?

Mme Jennifer Stoddart: Oui.

Je pense que, selon les gens à qui on s'adresse, les enfants à l'école, les parents, les jeunes adultes ou les aînés qui n'y connaissent à peu près rien, un certain nombre d'acteurs fédéraux et provinciaux partout au Canada s'occupent des questions de culture numérique.

Nous participons aux efforts dans la mesure où nos ressources le permettent. Dans le cadre du Réseau Éducation-Médias, nous venons de lancer un outil d'orientation sur les applications mobiles pour le personnel des commissions scolaires partout au Canada.

Il y a un certain nombre d'acteurs. Nous pouvons en faire plus, mais nous voulions porter cet outil à votre attention.

[*Français*]

Le président: Merci, madame Davidson. Votre temps est écoulé.

Je cède maintenant la parole à M. Andrews.

[*Traduction*]

M. Scott Andrews: Merci.

Bienvenue aux témoins. Nous sommes heureux de vous accueillir de nouveau.

Je demande toujours aux témoins dans cette étude ce qui constitue selon eux des renseignements personnels. Je pense que le principal organisme de protection de la vie privée que les entreprises, qui sont surtout américaines, craignent et écoutent, c'est la FTC. Je dirais qu'elles n'ont qu'un respect de façade pour les autres organismes, n'est-ce pas?

Les efforts investis par les organismes d'autres pays ou par le vôtre amènent-ils ces compagnies à apporter des modifications et à respecter les normes les plus élevées? Ou les compagnies ne font-elles que le minimum exigé par la FTC?

Mme Jennifer Stoddart: Les compagnies américaines, qui sont les principaux acteurs sur Internet, tiennent certainement compte de l'opinion de la FTC.

Je demanderais à la commissaire adjointe, Chantal Bernier, qui dirige nos enquêtes au jour le jour, de vous donner un exemple récent. Je pense que vous dites vrai concernant la FTC et les autres commissariats à la vie privée.

Mme Chantal Bernier (commissaire adjointe à la protection de la vie privée, Commissariat à la protection de la vie privée du Canada): Merci, madame la commissaire.

Oui, je pense que cette déclaration est très éloquente.

Si vous avez suivi nos travaux dans les médias, vous vous rappellerez peut-être qu'en 2011, nous avons produit un rapport pour présenter nos conclusions sur Google WiFi. Nous avons constaté que, durant la mise en oeuvre de Street View, Google a, par accident selon ses représentants — et nous n'avons aucune preuve du contraire —, recueilli les renseignements personnels de Canadiens. Nous avons donné une année entière à Google pour qu'elle nous remette une vérification réalisée par un tiers. Nous voulions avoir la garantie que Google appliquait toutes nos recommandations.

L'échéance était le 20 mai. Durant notre réunion au début mai avec les représentants de l'entreprise, nous avons constaté que Google ne semblait même pas envisager de présenter la vérification par un tiers que nous avions clairement exigée dans notre lettre. Les représentants se sont excusés et ont demandé une prolongation. En juillet, ils nous ont envoyé une vérification par un tiers qui répondait, en fait, à une demande de la FTC.

Je pense que ces informations prouvent votre argument.

● (1645)

M. Scott Andrews: Comment pouvons-nous exiger l'application des recommandations? Que faut-il faire pour que les compagnies appliquent les normes du Canada ou de votre commissariat? Est-ce que la seule solution, c'est de les poursuivre et de leur imposer des sanctions?

Quelles mesures devons-nous prendre? Comment pouvons-nous exiger l'application de nos normes en matière de protection des renseignements personnels?

Mme Jennifer Stoddart: D'après ce que j'ai observé au fil des ans, je pense que c'est la seule façon d'attirer leur attention.

Les noms sont déjà dans le domaine public. De nos jours, les entreprises sont très différentes de celles qui existaient lorsque la LPRDE a été adoptée. Des avocats m'ont indiqué à maintes reprises au fil des ans qu'ils souhaitent davantage de sanctions. Ils étaient très heureux que je parle de sanctions, parce que leurs clients, externes dans le cas d'un cabinet ou internes — comme un PDG — pour les avocats au sein des entreprises, veulent connaître tous les risques liés au non-respect des dispositions réglementaires.

Les entreprises veulent connaître les conséquences qu'elles encourent si elles ne respectent pas les normes canadiennes en matière de vie privée. Durant notre enquête, elles peuvent tout simplement promettre de corriger le tir. C'est ce que prévoit la loi. Étant donné que je n'intenterai pas une poursuite en Cour fédérale si les compagnies font des promesses et que nous parvenons à un accord, les responsables relèguent le respect de normes au second plan.

Les avocats ne peuvent pas dire à leurs clients de porter attention à la loi canadienne sur la protection de la vie privée, parce que le non-respect de la loi n'entraîne pratiquement aucune conséquence. Les entreprises s'intéressent donc à d'autres questions que l'atteinte à la protection des données, dont nous avons parlé plus tôt.

M. Scott Andrews: Je veux reparler de l'atteinte à la protection des données, car c'est une demande minimale. Si nous imposons une sanction et que nous améliorons le droit canadien, comment les tribunaux pourront-ils appliquer la loi? Comment pourront-ils imposer des sanctions, si la plupart des entreprises viennent des États-Unis?

Comment pouvons-nous sanctionner les compagnies américaines? Comment allons-nous imposer des sanctions à ces entreprises si elles ne respectent pas nos normes?

Mme Jennifer Stoddart: Je pense que la Cour fédérale a déjà imposé des sanctions et que le critère juridique au Canada est réel et concret. Je pense que bien des entreprises sont concernées. Le critère juridique est assez clair et doit être respecté.

Nous pouvons imposer des sanctions aux compagnies en raison de leur comportement en matière de renseignements personnels des Canadiens. Je ne pense pas que l'application de la loi soit un problème. D'autres pays appliquent leurs lois contre des entreprises établies à l'étranger. Le libellé des lois a une influence, mais un des avantages de la LPRPDE — et je souligne seulement le manque de pouvoirs de contrainte —, c'est qu'elle est neutre dans la mesure où il y a un lien avec le Canada, peu importe où se situent le siège social de l'entreprise ou les serveurs, etc. Je pense qu'une reformulation de la loi peut régler la question.

M. Scott Andrews: Avez-vous songé à la gamme de sanctions appropriées que nous devons imposer?

Mme Jennifer Stoddart: Oui. Je pense qu'il serait intéressant pour vous d'examiner la gamme de sanctions que l'Union européenne envisage présentement. Les sanctions se divisent en trois catégories. Les plus sévères s'élèvent à 2 p. 100 des revenus mondiaux. Il y a des discussions là-dessus, etc., mais les sanctions imposées par la FTC sont comprises entre 20 et 25 millions de dollars...

M. Scott Andrews: La FTC est un modèle intéressant, parce que la protection des renseignements personnels n'est pas vraiment...

Mme Jennifer Stoddart: Oui...

M. Scott Andrews: C'est un moyen détourné, et...

Mme Jennifer Stoddart: C'est exact.

M. Scott Andrews: ... la FTC le reconnaît.

Mme Jennifer Stoddart: En effet.

M. Scott Andrews: Si l'entreprise n'éveille pas les soupçons... Je trouve que c'est étrange, mais je présume que c'est simplement le système qui s'applique là-bas.

Est-il seulement question de l'avis obligatoire d'atteinte à la protection des données? Parlons-en, parce que vous avez dit que cet avis doit constituer un minimum. À quelle hauteur devraient s'élever les sanctions minimales et maximales?

● (1650)

Mme Jennifer Stoddart: Je pense que les sanctions maximales de l'Union européenne... Je vous rappelle que notre objectif lors de l'adoption de la LPRPDE, c'était de respecter les normes de l'UE. À ce jour, 80 pays dans le monde ont adopté le modèle européen.

De mémoire, je dirais qu'une quinzaine de pays en dehors de l'UE respectent clairement les normes européennes. Le Canada est le premier pays qui a emboîté le pas. Nous devons continuer d'examiner le modèle européen. Il faut prévoir divers niveaux d'amendes qui vont de quelques milliers d'euros à des montants très élevés. L'entreprise visée peut être une petite entreprise locale et familiale qui ne veut pas respecter la loi ou une grande multinationale.

[*Français*]

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

Je cède maintenant la parole à M. Mayes.

[*Traduction*]

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

Mesdames, merci de votre présence aujourd'hui.

Je dois dire que notre étude m'a permis d'en savoir plus sur les réseaux sociaux et certains obstacles que vous rencontrez.

Vous avez parlé dans l'exposé de conservation, de consentement valable, de limitation de l'utilisation et de responsabilité.

Je dirais qu'il est très simple d'appliquer des lois ou des directives sur la conservation, le consentement valable et limitation de l'utilisation. Il faut préciser quelles sont les bonnes pratiques. Selon ce que je comprends des témoignages, la simplicité est importante pour l'utilisateur. Je pense que la vraie question et votre principal défi, c'est la responsabilité.

Pour que les fournisseurs adoptent un comportement responsable, la réglementation doit-elle se fonder sur les plaintes ou sur la surveillance?

Mme Jennifer Stoddart: La responsabilité est une particularité de la loi canadienne qui est devenue très populaire à l'échelle internationale, car elle englobe bien les obligations des entreprises en matière de protection de la vie privée. Je pense que, dans l'idéal, il serait très utile que la loi permette au Commissariat à la protection de la vie privée d'exiger que les entreprises montrent comment elles sont responsables. C'est pourquoi je vous invite instamment à réexaminer la LPRPDE. Ce deuxième examen s'impose depuis longtemps. Honorables députés, nous avons un document complet là-dessus que nous pouvons vous envoyer.

En gros, il faudrait que les entreprises décrivent toutes les mesures qu'elles prennent pour respecter la loi en matière de protection de la vie privée. Par exemple, la compagnie peut avoir un chef de la protection de la vie privée, donner de la formation à son personnel, supprimer les données après le délai requis, investir dans la protection des données personnelles, montrer qu'elle applique la procédure appropriée pour répondre aux demandes présentées en vertu de la loi, etc. La responsabilité concerne toutes les obligations prévues par la loi.

De nos jours, si nous effectuons une vérification ou une enquête en raison d'une plainte, nous examinons de quelle manière la compagnie est responsable. Mais aucune disposition n'indique que l'entreprise doit montrer elle-même comment elle est responsable.

M. Colin Mayes: Le témoin précédent a dit quelque chose que j'ai trouvé fort intéressant. Il a indiqué que la plateforme est anonyme; ce n'est donc pas la protection des renseignements personnels qui est en jeu, mais celle du site utilisé pour accéder à la plateforme.

Je me demande donc qu'est-ce que nous protégeons ici. Est-ce la culture de protection de la vie privée? La pudeur et plusieurs aspects de ce que je juge privé ne sont plus ce qu'ils étaient il y a 10 ou 20 ans. La frontière se déplace-t-elle? Sur quoi se fonde ce que vous appelez la portée ou les principes de la vie privée?

Mme Jennifer Stoddart: En ce qui concerne la première question, monsieur le député, je n'ai pas entendu ce témoin. Je ne saisis pas très bien ce qu'il voulait dire. Nous pourrions peut-être consulter la transcription pour que je puisse vous donner une réponse à ce sujet.

M. Colin Mayes: Je pourrais prendre quelques instants pour vous expliquer ce qu'il en est. M. Calkins pourrait peut-être m'aider, car il connaît très bien cet aspect. Il a indiqué que l'information recueillie concerne le site et non la personne. Cette dernière pourrait communiquer des renseignements en cherchant un nouveau véhicule ou autre chose; ces renseignements sont enregistrés et vendus, ce qui permet aux vendeurs de véhicules d'implanter un témoin. Mais ce que j'appelle les renseignements vraiment personnels ne sont pas nécessairement communiqués. C'est l'information sur ce qui se passe sur le site qui est communiquée plutôt que les renseignements personnels.

● (1655)

Mme Jennifer Stoddart: D'accord. Oui.

M. Colin Mayes: Pouvez-vous faire la différence entre ces deux figures de cas, et aussi...

Mme Jennifer Stoddart: La culture de protection de la vie privée.

M. Colin Mayes: ... la culture de protection de la vie privée.

Mme Jennifer Stoddart: Je dirais à cet égard que oui, nous entendons souvent qu'ils ne veulent que savoir quels sites sont consultés. Mais nos propres travaux sur ce qu'on peut découvrir avec des témoins montrent que le problème, c'est qu'on peut colliger l'information sur tous les sites visités pour établir un profil. Dans certains cas, il est possible de découvrir le nom et l'adresse de la personne de sources publiques et ainsi établir, pour un citoyen ou un consommateur, un profil qui peut être juste ou totalement erroné.

Internet devient de plus en plus perfectionné, et le spécialiste américain Jeffrey Rosen a publié un excellent article à ce sujet il y a environ deux semaines.

La surveillance et la discrimination sur Internet posent un danger et un problème parce que quand on a visité un site, le serveur de publicité peut décider qu'on entre dans une certaine catégorie. Pour l'instant, nous ne pouvons tous avoir une catégorie qui nous est propre, mais disons qu'il s'agit d'une « femme d'âge moyen qui aime jouer au golf et conduire des voitures familiales ». Dans l'exemple américain, comme c'était des sites politiques qui avaient été visités, le message pourrait indiquer « votez ceci, pensez cela ». On peut faire mouche ou rater la cible.

Le fait que cette pratique déterminera l'information ou les publicités qui vous seront présentées et parfois, le classement dans les moteurs de recherche — mais je n'en suis pas certaine — signifie que l'expérience et l'étendue des connaissances que l'on a sur Internet seront limitées. Elles dépendront d'un profil qui peut être juste, erroné ou approximatif que des algorithmes vous attribuent.

On craint donc que certains soient classés dans des catégories artificielles et ne voient que les renseignements jugés appropriés pour cette dernière.

M. Colin Mayes: L'autre question portait sur les principes de ce que vous considérez comme la vie privée.

Mme Jennifer Stoddart: C'est une question extrêmement large, et la vie privée dépasse de loin mon mandat. Ce dernier se borne aux renseignements personnels détenus par le gouvernement ou des organisations.

Dans la LPRPDE, par exemple, nous mettons en oeuvre le code de l'Association canadienne de normalisation, qui figure en annexe de la loi et se fonde sur les travaux que l'OCDE a réalisés dans les années 1980.

M. Colin Mayes: Merci.

[*Français*]

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

Je cède maintenant la parole à M. Angus pour cinq minutes.

[*Traduction*]

M. Charlie Angus: Merci, Nous sommes heureux de vous revoir.

Notre premier témoin a tenu des propos intéressants, parlant de l'autoréglementation et de certains des acteurs qui oeuvrent au sein de l'industrie. Ils ont des normes, alors que d'autres n'en ont pas. Il a fait remarquer que l'autoréglementation fonctionne à merveille dans la mesure où on met en oeuvre un mécanisme d'application.

J'ai parfois l'impression que mes collègues du côté opposé considère que l'autoréglementation constitue une panacée. Si c'était le cas, la Somalie serait un centre de l'innovation internationale; or, elle ne l'est pas, parce qu'elle ne dispose pas de mécanisme d'application pour déterminer ce qui est une bonne ou une mauvaise activité.

En ce qui nous concerne, le mécanisme repose sur l'avis d'atteinte à la protection des données. C'est un des facteurs clés, selon moi. Si on accède à mes renseignements personnels, ce n'est pas pour connaître les sites que je visite, mes intérêts ou le terrain de golf que je fréquente, mais parce que j'utilise ma carte de crédit pour effectuer des achats. Si certains ont accès à ces renseignements, ma sécurité est menacée.

On trouve des termes intéressant dans la version reformulée que prépare le gouvernement. On parle de « risque réel », et non perçu, « de préjudice grave ». Si j'étais avocat de société, je dirais de ne révéler à personne qu'il y a eu atteinte à la protection des données. Qu'entend-on par risque important? Personne ne va venir vous tuer.

Il semble que le gouvernement fixe la barre si haute que les entreprises pourront se défiler et ne pas déclarer les atteintes à la protection des données, même s'il s'agit d'information sur les cartes de crédit ou de renseignements personnels, dont les cyberpirates sont friands. Devrait-on préciser le moment auquel une entreprise est tenue de révéler que des pirates informatiques ont mis la main sur des données personnelles?

Mme Jennifer Stoddart: Je crois, monsieur le député, que nous devons réexaminer cette question, et c'est pourquoi j'ai parlé au sous-ministre de l'Industrie. Je crois que l'ébauche de la mesure législative a été préparée il y a deux ou trois ans en fonction de nos connaissances d'alors. Nous devons réexaminer les lois, leur application et leurs effets néfastes sur les consommateurs. Certains ont demandé si la barre n'était pas fixée trop haut, compte tenu de la fréquence des atteintes à la protection des données, et je crois que cette question mérite non seulement qu'on la pose de nouveau, mais qu'on l'étudie et y réponde également.

● (1700)

M. Charlie Angus: Pour ce qui est de laisser le marché s'autoréglementer, nous avons fixé la barre extrêmement haute, ce qui fait que bien des choses peuvent se faufiler en-dessous en l'absence de mécanisme d'application. Je constate, à vous entendre, que nous allons nous retrouver loin derrière les autres pays occidentaux à ce chapitre.

J'ignore si la comparaison est juste, mais dans le débat sur le droit d'auteur, d'aucuns ont déploré que le Canada est le paradis des pirates parce qu'il ne dispose pas de mécanisme d'application. Je crois que certains propos étaient un peu exagérés. Mais s'il se produit une atteinte à la protection des données dans le marché actuel, les coupables n'ont rien à craindre, car personne n'interviendra, et si on entreprend des démarches, que peut-on faire contre des gens qui sont au-delà de la honte?

Certaines entreprises préféreraient peut-être s'établir au Canada pour poursuivre leurs activités en toute quiétude sous le régime des lois canadiennes, parce qu'elles se font rappeler à l'ordre en Angleterre, dans l'Union européenne et aux États-Unis.

Comme nous avons toujours fait figure de chef de file mondiale, ne devrions-nous pas établir des normes semblables pour être à la hauteur des autres pays occidentaux?

Mme Jennifer Stoddart: Je croirais que si, et je reste préoccupée par le fait qu'il n'existe pas de loi sur l'atteinte à la protection des données au pays, sauf en Alberta.

M. Charlie Angus: De plus, il semble étrange que certaines provinces aient des dispositions en la matière et d'autres pas. Avec la balkanisation des règlements relatifs à la protection de la vie privée, il suffit de trouver l'endroit où la situation est la plus facile et de s'y installer. Est-ce là le genre de norme d'innovation que nous voulons? Si vous êtes un cyberpirate, venez ici, mais si vous êtes une entreprise novatrice et respectée... En Europe et aux États-Unis, les entreprises savent que si elles respectent les règles du jeu, elles attireront des clients, alors que si elles trichent, elles se feront pincer.

N'est-il pas important d'instaurer une norme nationale au lieu d'une panoplie de régimes provinciaux?

Mme Jennifer Stoddart: Eh bien, je ne peux me prononcer pour les provinces, qui s'occupent de ce qui relève de leurs compétences, mais à titre de commissaire fédérale à la protection de la vie privée, je trouve particulièrement préoccupant que le gouvernement fédéral n'ait pas de dispositions relatives à l'atteinte à la protection des données pour les entités qui relèvent de son autorité, comme les banques. Nous savons que ces dernières sont des cibles favorites des pirates informatiques.

[*Français*]

Le président: Merci, monsieur Angus. Malheureusement, votre temps est écoulé.

Je cède maintenant la parole à M. Calkins pour cinq minutes.

[*Traduction*]

M. Blaine Calkins: Merci.

Je n'ai qu'une question, après quoi je laisserai le temps qu'il me reste à un de mes collègues.

C'est une question sur la capacité d'imposer des sanctions administratives, madame la commissaire. Vous avez souvent évoqué le modèle européen, dont l'échelle est établie en fonction de la taille de l'entreprise concernée.

Que pourriez-vous faire et quelles mesures seraient considérées comme équitables, outre l'application régulière de la loi dans le système judiciaire? Advenant une atteinte grave à la protection des renseignements personnels d'un citoyen, que ce soit dans une institution bancaire ou ailleurs, de quel ordre serait la sanction que vous devriez pouvoir infliger afin d'imposer une amende assez élevée pour décourager ou punir adéquatement une société multimilliardaire comme Google ou Facebook?

Mme Jennifer Stoddart: Merci de me poser la question.

Je ne me suis pas penchée sur le montant des amendes à imposer en cas d'atteinte à la protection des données, une infraction différente du simple fait de ne pas obéir à la loi sur le consentement lors de la communication de renseignements personnels.

Quand j'ai traité des amendes aux États-Unis, j'ai fait remarquer que le montant dépend du fait qu'en général, on respecte ou pas la loi, qu'on est en présence d'une atteinte à la protection des données et du fait que cette atteinte est attribuable à un manque d'investissement dans la sécurité. C'est une situation que nous avons vue à maintes reprises.

Selon moi, Industrie Canada, qui a élaboré la mesure législative, est le mieux placé pour examiner ce qui constituerait une amende adéquate. Tout ce que je veux faire remarquer — et je ne suis pas venue préparée pour en parler, mais la question a été abordée —, c'est qu'il faut imposer une sanction appropriée. Je ne saurais dire de quel ordre elle serait, mais je ne crois pas que nous devrions aller de l'avant avec cette partie du projet de loi C-12 à cet égard, si ce dernier accuse un tel retard par rapport aux normes internationales.

● (1705)

[*Français*]

Le président: Monsieur Dreeshen, vous pouvez continuer.

[*Traduction*]

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

Je n'ai que quelques remarques à formuler, ayant eu l'occasion de parler à diverses entreprises qui s'intéressent à la question.

L'un des aspects qui me préoccupent quand on fixe la barre relativement haut — et je crois que vous avez énuméré une liste en disant que chaque entreprise devrait disposer d'employés de divers niveaux pour protéger adéquatement les données —, c'est s'il ne faut pas craindre ensuite de commencer à faire des gagnants et des perdants. Peut-être que les grandes entreprises, qui disposent déjà de ce mécanisme, peuvent l'élargir. Les petites entreprises sauront alors qu'elles doivent respecter toutes les dispositions de la loi sur la protection des renseignements personnels.

C'est donc ce qui me préoccupe, quand les petites entreprises entrent en jeu. C'est quelque chose qu'on nous dit d'emblée: si on applique immédiatement des règles trop strictes, seules les entreprises assez costaudes pour supporter le fardeau qui leur est imposé réussiront à les respecter. Ce n'est pas ainsi qu'on favorise l'innovation.

Quand vous examinerez certaines de vos propositions — comme vous le ferez certainement, quand on pense à l'objet de notre étude —, je me demande si vous pourriez le faire en tenant compte de ce fait particulier, car nous voulons nous assurer de ne pas étouffer l'innovation. Voilà mes premières impressions et observations à ce sujet.

Nous avons également tenté de parler avec les personnes qui ont comparu du fait que ce n'est pas donné. Quand il est question d'utiliser le BlackBerry pour accomplir toutes sortes de fonctions, on se retrouve tout à coup libre de faire tout ce qu'on veut, protégé de soi-même, en fonction de certaines de ses activités. J'examine la question sous cet angle.

Si on entre dans un commerce et qu'on commence à lire une revue sur place, viendra un moment où il faudra la payer; il faut reconnaître que cela s'inscrit dans nos pratiques. C'est un fait que peu d'organismes de réglementation reconnaissent vraiment. Mais quand on demande aux entreprises comment elles font de l'argent et ce qu'elles font, on comprend un peu mieux ce qu'il en est.

S'il me reste quelques secondes, j'aimerais terminer en parlant du droit à l'oubli. Parmi les analogies que nous avons entendues figure celle de la personne qui verse un verre d'eau dans une rivière et, quand l'eau s'est écoulée, voudrait ravoir son verre d'eau alors que l'eau a descendu le cours de la rivière pour se perdre dans l'océan.

Il y a divers avis à ce sujet. Je me demande si vous pourriez réagir à certains de mes propos dans le temps qu'il me reste.

Mme Jennifer Stoddart: Je comprends, monsieur le député...

[*Français*]

Le président: Je m'excuse de vous interrompre. Le temps est écoulé, mais je vais vous laisser environ une minute pour répondre.

Mme Jennifer Stoddart: Avez-vous dit trois minutes?

Le président: Je vous accorde environ une minute.

[*Traduction*]

Mme Jennifer Stoddart: D'accord.

Je dirais alors très brièvement que tout d'abord, nous avons toujours essayé d'adapter la loi aux petites et moyennes entreprises. Certains des exemples que j'ai donnés concernent les sociétés de très grande envergure et non les petites et moyennes entreprises.

Pour ce qui est ensuite d'étouffer l'innovation, je ne considère pas que cette dernière a toujours un lien direct avec la protection de la vie privée. Elle est, selon moi, principalement encouragée par la formation de capital, le capital entrepreneurial, qui est gratuit, et les niveaux d'instruction ou de connaissances techniques.

De plus, le commissariat n'a rien contre le fait que les gens vendent leurs renseignements personnels pour obtenir des services gratuits. Nous n'avons jamais rien dit de pareil. Nous n'avons aucun problème à l'égard du modèle Internet. Nous voulons simplement que la loi que le Parlement a adoptée en 1999 soit appliquée correctement: les gens doivent donner leur consentement, et comprendre ce qu'ils vendent et l'usage qui en sera fait.

Pour ce qui est enfin du droit à l'oubli, je considère qu'il s'agit d'un concept important. Nous devons examiner sérieusement la manière et les moyens de l'appliquer. Le Parlement a eu la sagesse de dire qu'en vertu de la LPRPDE, les gens ont le droit de faire disparaître leurs renseignements personnels; en un certain sens, nous disposons déjà d'un mécanisme. Nous avons toutefois de gros problèmes avec certaines entreprises qui n'ont prévu aucun mécanisme pour effacer les renseignements des jeunes.

[*Français*]

Le président: Je vous remercie de votre réponse.

Je cède la parole à M. Boulerice. Il dispose de cinq minutes.

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

Madame la commissaire, mesdames, je vous remercie d'être ici avec nous.

Comme le disait ma collègue, il est intéressant de vous recevoir au début du processus et à la fin. Je prendrai quelques secondes pour dire que cette étude, grâce à ma collègue, a un peu été une révélation pour moi. Cela m'a ouvert les yeux sur le fait qu'on est beaucoup plus suivis qu'on ne le pense sur Internet et les médias sociaux. J'ignorais à quel point on était suivis et observés.

J'ai l'impression que c'est le cas pour beaucoup de mes concitoyens qui, rapidement, acceptent les conditions et, par la suite, vont naviguer et se promener sur les sites. Ils ne réalisent pas la machine qui existe, que ce soit les *browsers* les Google, les médias sociaux ou que ce soit ces *data brokers* dont j'ignorais même l'existence il n'y a pas si longtemps. Ils recueillent un foule d'informations sur nous, nos habitudes, nos choix, nos préférences, les lieux qu'on fréquente, nos achats, nos idées. Par la suite, ils vont regrouper tout cela, feront des ensembles et, souvent, vendront ces informations. Je pense que dans ce que vous nous avez dit, le rôle d'éducateur — que vous devriez jouer davantage — est à mon sens aussi important que celui de pouvoir imposer des amendes ou des pénalités.

J'aimerais que vous me parliez de votre perception de la connaissance numérique ou de la littératie numérique chez nos concitoyens canadiens. Les gens savent-ils qu'ils sont aussi suivis que ça?

● (1710)

Mme Jennifer Stoddart: Nous faisons des sondages tous les ans. Une année, c'est auprès des entreprises, l'année suivante, c'est auprès des citoyens. Les Canadiens sont très préoccupés par leur vie privée, ils pensent que c'est un des enjeux majeurs de l'avenir. Si je ne me trompe pas, 40 % des gens que nous avons sondés identifient Internet comme la source possible d'une violation de leur vie privée. En général, il y a un malaise relativement à la surveillance explicite par les caméras vidéo ou quand on navigue sur le Web, mais les gens ne sont pas très informés parce que c'est compliqué à comprendre.

M. Alexandre Boulerice: Vous avez dit que le projet de loi qui a été déposée à la Chambre a maintenant deux ou trois ans d'existence, mais qu'il n'a pas été adopté. Il faudrait peut-être revoir tout cela et revoir certaines dispositions parce que l'univers informatique et Internet ont changé depuis ce temps. Vous nous avez dit qu'il y a des risques à l'inaction et que si on ne fait rien, on va accuser du retard par rapport aux autres pays occidentaux. J'aimerais savoir, selon vous, quelle est la conséquence de notre possible inaction sur la protection de la vie privée des citoyens canadiens. En quoi cela aura-t-il un impact sur les gens?

Mme Jennifer Stoddart: Je trouve inadmissible qu'au Canada en 2012 , nous n'ayons pas, sauf en Alberta, de protection législative contre les fuites de données. Une fois par semaine environ, des compagnies ou le gouvernement lui-même soumettent à notre bureau des dénonciations volontaires de fuites qui affectent des milliers de citoyens et de consommateurs.

Aux États-Unis, 49 des 51 États appliquent une protection législative ou des mesures dissuasives. Cela ne consiste pas uniquement à dissuader les entreprises. On les oblige également à faire gratuitement une évaluation de la cote de crédit. Un an plus tard, elles doivent vérifier si les gens subissent les effets de la fuite de données et, le cas échéant, réparer les dommages causés par celle-ci.

Le fait que les Canadiens ne bénéficient pas de cette protection me semble grave et j'espère bien que le gouvernement va très bientôt présenter des mesures législatives à ce sujet.

M. Alexandre Boulerice: Surtout dans le secteur bancaire, où tout le monde aurait intérêt à ce que ce soit plus réglementé, pour des raisons assez évidentes.

Mme Jennifer Stoddart: Exactement.

M. Alexandre Boulerice: Est-ce qu'il me reste un peu de temps?

Le président: Il vous reste 30 secondes.

M. Alexandre Boulerice: Vous êtes bien généreux, monsieur le président.

Selon vous, l'autoréglementation du secteur Internet et des médias sociaux est-elle suffisante? On a discuté, dans le cadre du témoignage précédent, des règles volontaires harmonisées, mais quand on parle aux gens de l'industrie, on a l'impression qu'aucun mécanisme de surveillance adéquat n'est prévu.

Laisser ces gens se réunir pour décider de leur mode de fonctionnement, sans que personne ne les surveille, est-il suffisant?

● (1715)

Mme Jennifer Stoddart: Non, je n'y crois pas. Cette approche ne fonctionne pas. Depuis quelques années aux États-Unis, toute l'industrie de la publicité est en pourparlers à ce sujet, mais sans succès. Ces gens n'arrivent pas à s'entendre sur la façon de s'autoréglementer. L'autoréglementation, c'est bien, mais je pense qu'il faut une loi pour l'appuyer. Comme ça n'a pas fonctionné pour les Américains, il est possible qu'ils établissent une loi.

M. Alexandre Boulerice: Merci.

Le président: Merci, monsieur Boulerice.

Je remercie la commissaire d'être venue témoigner devant nous aujourd'hui. C'est, à toute fin pratique, ce qui met fin aux témoignages dans le cadre de cette étude.

Nous allons faire une pause de quelques minutes pour ensuite discuter des travaux futurs du comité.

Mme Jennifer Stoddart: Merci.

Le président: Comme vous le savez, il va falloir se trouver quelque chose à faire au retour, après les Fêtes.

Mme Jennifer Stoddart: Merci beaucoup, monsieur le président.

Je veux aussi remercier tous les membres du comité.

[*Traduction*]

Je vous remercie beaucoup de porter un tel intérêt à cette question. C'est, je crois, l'étude parlementaire la plus importante que nous ayons vue depuis longtemps sur la protection de la vie privée. J'aimerais simplement vous dire à quel point le commissariat reconnaît le mérite de votre travail.

Merci.

● (1715)

(Pause)

● (1715)

[*Français*]

Le président: À l'ordre, s'il vous plaît.

Nous abordons maintenant les travaux futurs du comité. Monsieur Warkentin, vous avez la parole.

[*Traduction*]

M. Chris Warkentin (Peace River, PCC): Pourrais-je présenter une motion pour déclarer le huis clos? Il y a un certain nombre de questions dont nous voudrions tous parler, je crois, mais elles concernent les travaux futurs au comité. Il me semble qu'il serait plus efficace d'en discuter à huis clos.

[*Français*]

Le président: Une motion voulant que nous poursuivions la séance à huis clos est soumise et on demande que le vote se fasse par appel nominal. Je vais laisser le greffier procéder au vote.

(La motion est adoptée par neuf voix contre deux.)

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