CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la justice et des droits de la personne

JUST • NUMÉRO 029 • 2e SESSION • 41e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 5 juin 2014

Président

M. Mike Wallace

Comité permanent de la justice et des droits de la personne

Le jeudi 5 juin 2014

● (1105)

[*Traduction*]

Le président (M. Mike Wallace (Burlington, PCC)): J'ouvre la 29e séance du Comité permanent de la justice et des droits de la personne. La séance est télévisée.

Selon l'ordre du jour du lundi 28 avril 2014, nous poursuivons notre étude du projet de loi C-13, Loi modifiant le Code criminel, la Loi sur la preuve au Canada, la Loi sur la concurrence et la Loi sur l'entraide juridique en matière criminelle.

Nous recevons des témoins ce matin. Je veux m'excuser à l'avance: nous avons commencé un peu en retard, car nous votions.

Je rappellerai au comité que nous avons discuté des votes la dernière fois, afin que nous puissions être télévisés et avoir des témoins par vidéoconférence. Nous allons poursuivre quelques minutes même lorsque le timbre sonnera. Suite aux remontrances du Président de la Chambre, nous n'allons pas poursuivre trop longtemps, mais un peu quand même.

Cela dit, je veux remercier nos invités.

Pour aller plus vite, je passerai directement aux témoins.

Notre premier témoin est M. Kempton de l'Anti-Bullying Initiative.

Vous avez 10 minutes, monsieur. La parole est à vous.

M. Roy Kempton (coordonnateur, Anti-Bullying Initiative): Merci monsieur le président et membres du comité. Merci de me donner l'occasion de m'adresser à vous au sujet du projet de loi C-13 et de partager avec vous ce qu'a vécu ma famille au cours des cinq dernières années à cause de l'intimidation.

Je m'appelle Roy Kempton et je vis à l'est de Cobourg dans le comté de Northumberland. En janvier 2008, j'ai pris ma retraite après 41 ans comme ingénieur professionnel et j'avais hâte de passer de belles années en m'adonnant à la poésie et au golf.

Sept mois après le début de ma retraite, ma petite-fille, Abigayle Kempton, s'est pendue dans la cour arrière de sa maison sur la rue Harwood Road, à Baltimore en Ontario, deux semaines après son 14e anniversaire. Je ressens toujours les frissons de cet appel téléphonique. En perdant mon unique petite-fille, j'ai perdu aussi cet amour spécial que partage un grand-père et sa petite-fille et notre passion commune pour l'écriture. Imaginez alors ce que ses parents ont ressenti — le vide, les doutes.

Comme toutes les familles qui font face à de tels traumatismes, nous avons été submergés d'émotions. Nous avons appris dans sa lettre finale qu'elle avait été victime d'intimidation verbale et en ligne et que, comme elle l'a écrit, « elle voulait la paix et la fin de ses souffrances. » Elle n'avait jamais vraiment parlé de l'intimidation. Nous avons mal compris ses sautes d'humeur, les voyant comme les vicissitudes de l'adolescence. Sachant les souffrances causées par l'intimidation, nous sommes fiers qu'elle ait été au tableau d'honneur de la 8e année.

Elle a supprimé tous les messages blessants de son téléphone cellulaire et de sa page Facebook. Les policiers nous ont dit qu'on pouvait les retrouver. Nous ne l'avons pas voulu. Nous avons pensé qu'on y gagnerait seulement que plus de douleur. Nous avons décidé de canaliser nos énergies vers une approche positive, qui nous permettrait de voir de bonnes choses découler de ce drame. Nous avons fait ce choix en pensant à Abigayle, une personne sensible et bienveillante au merveilleux sens de l'humour et aux rires joyeux.

Nous avons appris de ses amis les mauvais traitements qu'elle a subis. Encore plus étrange selon moi, ceux qui l'ont intimidé l'ont admis, laissant une note signée sur sa tombe demandant son pardon. Accompagnée de sa mère, l'une d'entre elles m'a fait part de ses remords, et j'ai compris qu'il pouvait y avoir des victimes des deux côtés de ce fléau éternel. Elle m'a dit qu'elle était responsable de la mort d'Abi. Elle pleurait alors que sa mère me parlait de sa dépression, de ses idées suicidaires et de son hospitalisation. J'ai pleuré avec elle et je me suis dit que tout cela était très triste et insensé. Elle n'était qu'une enfant, comme ma petite-fille. Je n'ai pas vu un tyran, mais une pauvre et triste jeune fille qui essayait de gérer son trop plein d'émotions. Ce n'était pas le temps des représailles ou de la justice, ou quel que soit le nom que l'on veuille donner à ces choses.

Nous devions faire quelque chose pour éviter que de tels drames se reproduisent. Nous avons pensé à une bourse au nom d'Abi à l'école secondaire où elle voulait étudier. Il est devenu évident que nous devions en faire plus, étant donné l'appui de nos amis et de la communauté en général. En mai 2009, nous avons fondé ABI, une initiative pour combattre l'intimidation qui utilise l'acronyme de son nom. Elle planifiait d'étudier l'animation au collège, et c'est l'un des personnages qu'elle a créés que nous utilisons pour symboliser notre programme.

Notre initiative essaie de souligner les conséquences tragiques de l'intimidation auprès des élèves du primaire et du secondaire. Nous avons créé un site Web et une page Facebook pour rejoindre un plus vaste public. Nous publions également un bulletin de nouvelles.

Sans formation professionnelle, mais parlant du coeur, nous avons fait des exposés dans des écoles primaires, des écoles secondaires, des églises, des conseils locaux et des comités du conseil, des camps de scout, et des camps de jour. Nous avons rencontré des familles chez elles, et nous avons aidé des parents et des élèves en personne. Nous avons organisé des rassemblements pour faire la promotion de la sensibilisation. Nous avons fait l'objet de plusieurs articles dans les journaux locaux.

● (1110)

Cette année marque le cinquième anniversaire de notre initiative. À la fin de cette année scolaire, nous aurons offert 15 000 $ en bourses à des étudiants ayant réussi leur 12e année et qui ont fait preuve de leadership exceptionnel pour combattre l'intimidation dans leur école et dans la communauté en général. Nous dirigeons également un programme à l'école primaire où nous présentons des t-shirts, des épinglettes, des bracelets, etc., aux étudiants méritants choisis par le personnel de l'école. Nous travaillons actuellement avec des groupes communautaires et des représentants des conseils scolaires pour que l'histoire d'Abi soit présentée dans d'autres d'écoles.

Nous espérons pouvoir changer les choses en présentant nos expériences. Nous croyons que rejoindre les élèves lorsqu'ils sont jeunes constitue la clé pour développer de meilleures compétences et comportements sociaux. Cela commence vraiment dans la famille, où on devrait enseigner le respect d'autrui.

Arrivons-nous à changer les choses? En jugeant par les courriels, les lettres et les encouragements verbaux reçus, la communauté croit que oui. Nous savons qu'il y a des groupes qui ont des programmes et qui font un travail énorme pour aider les enfants à vivre et à apprendre dans des environnements sécuritaires. Nous savons aussi qu'il y aura toujours des personnes qui contourneront les normes de bonne conduite qui pourraient justifier des enquêtes criminelles.

Comme mon ami Grahame Woods l'a écrit récemment dans le *Northumberland Today*:

> Jadis, lorsque j'étais enfant, on entendait dans la cour d'école le proverbe « La bave du crapaud n'atteint pas la blanche colombe ». Oh, à quel point était-ce faux! C'était un monde où on communiquait par la voix, les lettres, le téléphone (pour certains) ou même le code morse. Oui, aujourd'hui, il y a toujours l'intimidation verbale idiote, mais la bave mortelle lancée dans l'espace en pressant « Envoyer » de façon irréfléchie — de façon irrécupérable, causant des dommages émotionnels invisibles jusqu'à ce que le destinataire ne puisse plus le supporter.

Rappelez-vous que ce sont les grands-parents et les parents qui mettent cette arme dans les mains des enfants sous forme d'appareils mobiles, Facebook, Twitter et les autres médias sociaux. Et puis nous nous démenons pour protéger nos enfants.

La loi se rend utile, mais au bout du compte, ce sont les familles qui doivent être vigilantes dans un monde où nous avons tous de la difficulté à suivre l'évolution de la technologie. Les enfants devraient connaître les conséquences d'une mauvaise utilisation de ces appareils. Le regret ne peut pas effacer les conséquences émotionnelles des mots et des images blessants envoyés anonymement en pressant un bouton.

Je doute que les événements entourant la mort de ma petite-fille soient couverts par les dispositions du projet de loi C-13. Elle a subi l'intimidation de ceux qu'elle avait considérés des amis. C'était de la torture classique de cour d'école avec la technologie moderne. Quand même, je comprends qu'on ait besoin de cette loi et je crois qu'elle pourra protéger ceux qui sont menacés par des activités en ligne.

La technologie peut nous enlever nos moments de repos paisibles. Notre amour d'Internet a malheureusement miné la chose même que nous voulons chérir lorsque, tristement, dans certains cas, il est trop tard. À 14 ans, je pouvais me sauver dans un long chemin bordé de hautes haies qui menait vers la maison de la ferme où nous vivions, sur une colline entourée d'arbres, sans téléphone ou boîte aux lettres. Ce genre d'intimité semblait provenir d'un autre monde, un monde qu'on ne peut seulement qu'imaginer aujourd'hui.

J'espère que mon exposé reflétera l'énergie dont Abi a fait preuve dans sa courte, mais très belle vie. Dans un monde imparfait, si elle avait des rêves de perfection, c'était sûrement d'être acceptée et respectée telle qu'elle était, avec les mêmes défauts que nous avons tous. Le respect des autres est au coeur de cette initiative. Voilà ce que nous a enseigné cette enfant. Voilà ce que nous devrions enseigner aux nôtres.

Merci.

● (1115)

Le président: Monsieur Kempton, merci beaucoup pour votre exposé.

Le prochain exposé vient de la Canadian Crime Victim Foundation.

Monsieur Wamback, vous avez la parole pendant 10 minutes.

M. Joseph Wamback (fondateur et président, Canadian Crime Victim Foundation): Merci, monsieur le président et membres du comité.

Je suis ravi d'être ici aujourd'hui pour témoigner et participer à l'achèvement de cette initiative. Je suis reconnaissant de voir un appui politique de tous les partis à ce projet de loi. Pour moi, les gens avec qui je travaille et les centaines de milliers de Canadiens, le plus tôt le projet de loi C-13 recevra la sanction royale, le mieux ce sera.

Cela ne concerne pas seulement les jeunes, mais tous les Canadiens. Le projet de loi C-13 traite de notre croyance essentielle que la vie et l'avenir des victimes de cyberintimidation et d'activités criminelles électroniques sont importantes et que nous, les Canadiens, reconnaissons cette importance. Je ne pense pas que qui que ce soit dans ce comité ait sous-estimé les effets horribles de la cyberintimidation sur les Canadiens, surtout nos jeunes.

J'aimerais que l'on puisse légiférer les bonnes compétences parentales, mais comme nous le savons tous, c'est impossible. Je crois également que le projet de loi C-13 ne constitue pas une fin. C'est un début. Nous devons continuer d'informer nos jeunes sur les effets transformateurs de l'intimidation par Internet et, ce qui est tout aussi important, sur les conséquences et les sanctions qu'amène ce comportement. Je crois fermement qu'appliquer des conséquences est la première étape vers la prévention. Le projet de loi C-13 est un début et pour qu'il soit efficace, cette initiative doit être transparente, prévisible, et surtout, perçue comme telle par tous les Canadiens. C'est pourquoi je crois que l'application et l'aspect logistique de la loi sont aussi importants et je suis ravi de constater que tout cela est traité en détail dans le projet de loi.

Je l'ai examiné en détail et je suis convaincu qu'il n'y aura pas d'empiètement sur nos droits personnels à la protection de la vie privée. Je ne crois pas que les policiers ou l'État menacent l'existence de ma liberté, ni celle des autres Canadiens. Je ne m'inquiète pas des ordonnances de préservation ou de communication, tout comme les parents des victimes à qui j'ai parlé récemment ne s'en inquiètent pas non plus. Je pense que le tollé entourant les atteintes à la vie privée vient de ceux qui n'ont pas lu ou compris les dispositions du projet de loi C-13 — ou ils sont tout simplement de mauvaise foi.

Je me suis toujours inquiété de la perte de confiance envers le système judiciaire, surtout de la part de nos jeunes. Perdre confiance envers le système et croire qu'il est injuste menace la confiance envers les tribunaux et cela a des conséquences dangereuses, y compris le fait de ne pas rapporter ce genre d'activités criminelles. Je crois fermement que le dépôt du projet de loi C_13 démontrera à ceux qui sont marginalisés et isolés par la cyberintimidation, surtout nos jeunes, que nous nous en préoccupons et que nous sommes prêts à les protéger et à faire respecter cette loi. Si nous ne le faisons pas, cela minera son efficacité et notre capacité collective de réduire la fréquence de ce genre d'activités criminelles dévastatrices.

L'intimidation et la cyberintimidation ne se limitent pas à la distribution d'images intimes sans le consentement d'une personne. Les victimes déclarent également qu'il est impossible d'échapper à la distribution électronique de la haine et de la cyberintimidation, qui comprend les menaces, la propagation de fausses rumeurs, la vengeance et, encore plus important, le rejet social. C'est impossible à cause de la nature publique d'Internet. Les effets transforment la vie et certains y perdent même leur avenir, ce qui nous touche tous.

Après un examen minutieux, j'ai trois recommandations pour le comité. Premièrement, et je suis certain qu'on y a pensé, mais je n'ai pas pu trouver de référence à la Loi sur le système de justice pénale pour les adolescents dans l'administration du projet de loi C-13. Puisque ce projet de loi vise les jeunes, je propose que les amendements appropriés s'appliquent également à la Loi sur le système de justice pénale pour les adolescents en matière d'application, d'enquête et de sanctions.

Deuxièmement, je crois que pour réussir, nous aurons besoin de continuellement faire de l'éducation sur les détails et les conséquences de la cyberintimidation. Cela doit être régulièrement présenté et compris par tous les Canadiens, surtout les jeunes, afin qu'ils soient conscients des effets nocifs, et surtout, des conséquences de la cyberintimidation. On doit rappeler à tous les Canadiens, et surtout nos jeunes, que l'anonymat n'existe pas sur Internet et qu'il doit y avoir des conséquences, cohérentes et prévisibles, associées à ce comportement.

● (1120)

Après les agressions envers mon fils en 1999, et pendant plusieurs années, ma famille a reçu des courriels contenant des menaces de mort et des messages accusatoires complètement dégoûtants sur les blogues et les médias sociaux insultant ma famille et mes efforts pour aider les victimes de crime et demander des changements législatifs afin que le Canada soit un endroit plus sûr pour nos enfants.

Nous sommes toujours victimes de ces événements et on ne peut rien faire, car ces messages et courriels ont toujours été anonymes. Ces personnes aux intentions violentes sont toujours demeurées anonymes et leur courage à accuser et insulter a été protégé et renforcé par cet anonymat.

J'ai parlé à de nombreux enfants et familles victimes d'attaques anonymes et lâches semblables par Internet, et les résultats sont toujours les mêmes. Les menaces et la propagation de fausses informations, de rumeurs et d'accusations par voie électronique sont plus dévastatrices et écrasantes pour les victimes que si c'était fait en personne, à cause de la nature publique d'Internet. Ce n'est plus de personne à personne; tout le monde peut le voir.

J'ai donc une troisième recommandation, qui, je l'espère est encore une fois seulement de nature administrative, mais je pense qu'elle est nécessaire pour apporter une plus grande clarté, et surtout, une plus grande certitude.

Le projet de loi C-13,, tel qu'indiqué au paragraphe 18, fait référence aux articles 371 et 372 du Code criminel canadien, qui sont des infractions aux droits à la propriété. Cela devrait être élargi pour s'assurer que les autres infractions qui font référence à des technologies désuètes, comme le téléphone et le télégraphe, soient également mises à jour. Avec ces amendements, ces actes seraient punissables lorsqu'on utilise le courriel, les messages texte, les blogues, ou tout autre moyen de télécommunications et, surtout, cela donnerait aux autorités les mêmes pouvoirs en matière de procédures et d'enquêtes.

Ces articles couvrent ce qui suit: les infractions d'ordre sexuel; les actes contraires aux bonnes moeurs; l'inconduite, l'article 181 du Code criminel et les infractions contre la personne et la réputation, les articles 264 et 265 du Code criminel.

La cyberintimidation ou les activités criminelles distribuées ou perpétrées par voie électronique existent, car elles proviennent de personnes anonymes mal intentionnées dont l'identité est très difficile, sinon impossible, à retracer. Cela existe parce que les auteurs de ces actes croient que leur identité est secrète et qu'on ne pourra jamais leur demander de rendre des comptes, et j'espère que cela changera.

Nous ne pourrons jamais mettre fin au crime électronique ou à la cyberintimidation, mais je pense que cette initiative et les efforts d'éducation subséquents sensibiliseront la population aux effets des crimes en ligne et alerteront nos jeunes à ses effets dévastateurs sur leurs pairs.

J'espère également que cela imposera des conséquences et des sanctions graves pour ceux qui profitent de l'anonymat d'Internet pour intimider.

Merci beaucoup de m'avoir écouté.

● (1125)

Le président: Monsieur Wamback, merci pour cet exposé.

Le prochain témoin vient de l'Association canadienne des libertés civiles, Mme Cara Zwibel.

Mme Cara Zwibel (directrice, Programme libertés fondamentales, Association canadienne des libertés civiles): Merci, monsieur le président

Je m'appelle Cara Zwibel, et je suis avocate et directrice de programmes à l'Association canadienne des libertés civiles.

L'ACLC est une organisation nationale non partisane, non gouvernementale et à but non lucratif appuyée par des milliers de Canadiens de tous les milieux. Cette année, l'ACLC célèbre ses 50 années d'efforts pour protéger les droits et libertés de tous et en faire la promotion.

Dans notre rôle de défenseurs des droits fondamentaux, y compris la liberté d'expression, le droit à la vie privée et le droit d'être libre de toute ingérence déraisonnable de l'État, je suis reconnaissante d'avoir l'occasion de comparaître devant le comité et d'exprimer certaines de nos préoccupations concernant le projet de loi C-13.

Mes observations d'aujourd'hui porteront sur deux points principaux. Le premier, c'est la création de la nouvelle infraction de distribution non consensuelle d'images intimes. Nous croyons que cette infraction est conçue de manière trop générale et pourrait couvrir des activités légales d'une façon qui viole de façon déraisonnable la liberté d'expression.

Deuxièmement, je veux vous parler des nouveaux pouvoirs d'enquête prévus par le projet de loi. La majeure partie du projet de loi C-13 vise à accroître les pouvoirs d'enquête des policiers, et de façon qui touche non seulement les enquêtes en matière de cyberintimidation, mais aussi les enquêtes pour toutes les infractions couvertes par le code. Dans la mesure où on a constaté des lacunes dans les capacités des enquêteurs de s'occuper des crimes en ligne, de telles mesures sont certainement appropriées. Cependant, d'après nous, les dispositions du projet de loi C-13 ne trouvent pas le bon équilibre entre les besoins d'enquête et les droits personnels en matière de vie privée. Le projet de loi autorise des ingérences déraisonnables de la part de l'État dans la vie personnelle des Canadiens. L'ACLC ne peut pas appuyer le projet de loi sans des modifications importantes aux dispositions sur les pouvoirs d'enquête.

Je vais commencer avec la nouvelle infraction de distribution non consensuelle d'images intimes. Pour débuter sur ce sujet, je reconnais que la cyberintimidation est une préoccupation pour de nombreux Canadiens. L'ACLC partage l'opinion que des administrations locales, et les gouvernements provinciaux et fédéral ont un rôle à jouer pour régler ce problème. Il y a certainement des dommages réels et de graves ennuis qui découlent de la distribution d'images intimes. Mais le droit criminel est un outil grossier, et l'utiliser pour s'attaquer au problème de cyberintimidation peut mener à la criminalisation des victimes autant que des auteurs des actes en question.

Fondamentalement, cette nouvelle infraction criminalise l'expression. Même l'expression qui est blessante, gênante ou gravement insultante est protégée par la Charte canadienne des droits et libertés, et ne peut être limitée que de façon raisonnable et justifiable dans une société libre et démocratique. Les restrictions à l'expression devraient être strictement adaptées pour atteindre l'objectif visé. L'objectif dans ce cas est bon. Nous craignons que l'infraction ne soit pas strictement adaptée pour l'atteindre.

D'après nous, l'infraction proposée est trop générale et limite la liberté d'expression de diverses façons qui sont déraisonnables.

Premièrement, l'infraction n'exige pas une intention malveillante. Étant donné l'omniprésence des images intimes qui flottent dans le cyberespace, l'absence d'une exigence en matière d'intention malveillante signifie que des personnes pourraient être tenues criminellement responsables d'avoir affiché, partagé ou envoyé une image intime qui se trouve déjà en ligne, et qui a peut-être été initialement affichée par la personne représentée, ou qui représente quelqu'un qu'ils ne connaissent pas.

Deuxièmement, la définition d'image intime est trop vaste, et son utilisation par rapport à une attente raisonnable en matière de vie privée posera des défis aux tribunaux qui devront interpréter et appliquer la loi. Le concept d'attente raisonnable en matière de vie privée, utilisé pour expliquer le droit de ne pas être soumis à des fouilles et à des perquisitions abusives en vertu de l'article 8 de la Charte, est complexe. Dans le contexte de la jurisprudence au sujet de l'article 8 de la Charte, on parle des intérêts privés des personnes vis-à-vis de l'État. L'infraction proposée, cependant, traite plutôt des attentes en matière de vie privée que les gens ont vis-à-vis d'autres personnes ou de la société en général. Ce concept sera beaucoup plus difficile à interpréter et à appliquer lorsque les images en cause n'ont pas été créées par l'accusé et pourraient provenir de diverses sources. J'ai inclus plus de renseignements à ce sujet dans mon mémoire au comité.

Troisièmement, l'ACLC s'inquiète des ordonnances qui peuvent être imposées aux personnes condamnées en vertu de la nouvelle infraction, surtout des ordonnances qui empêchent le contrevenant d'utiliser Internet ou tout autre réseau numérique. Une telle restriction, qui selon le libellé actuel du projet de loi peut être imposée sans condition par rapport à sa portée ou à sa durée, est draconienne. Empêcher les personnes d'utiliser Internet peut avoir comme effet de les isoler de leurs amis et de leur famille, de limiter de façon importante leur capacité d'avoir accès à l'information et à communiquer avec le monde qui les entoure, et peut avoir des conséquences négatives sur leurs perspectives d'emploi ou d'éducation. L'ACLC croit que cet article devrait être grandement restreint. Telle que rédigée actuellement, la nouvelle infraction a une portée trop grande, et la norme d'insouciance utilisée est beaucoup trop faible pour une infraction qui criminalise une gamme aussi vaste d'expression.

● (1130)

J'aimerais maintenant parler des nouveaux pouvoirs d'enquête que comprend le projet de loi, puisqu'ils soulèvent de graves préoccupations, surtout dans le contexte des renseignements ayant récemment fait surface sur l'ampleur des renseignements personnels que les institutions gouvernementales demandent et reçoivent déjà des fournisseurs de services de télécommunications et d'Internet sans autorisation judiciaire préalable et sans que les clients le sachent ou y consentent.

Nous sommes ravis de voir que nombreuses des dispositions plus intrusives des incarnations précédentes des lois sur l'accès légal ont été mises de côté. Mais nous continuons de nous inquiéter de plusieurs aspects du projet de loi, et en particulier la disposition sur l'immunité qui se trouve au paragraphe 487.0195(1) et (2). Ces paragraphes visent à accorder l'immunité en matière criminelle ou civile à toute personne qui préserve des données ou qui fournit un document aux autorités policières lorsqu'il n'y a pas d'interdiction légale de le faire.

À première vue, cette disposition semble être redondante. Elle indique seulement qu'une personne ne peut pas être poursuivie pour quelque chose qui n'est pas interdit par la loi. Le ministre a dit que cet article n'apporte rien de nouveau et qu'il est là seulement pour clarifier la situation. J'ai également suivi les séances du comité à ce sujet et j'ai compris que de nombreux membres du comité continuent de croire que cette disposition est totalement inoffensive.

Je ne suis pas d'accord avec cette description et je recommande au comité de ne pas permettre à cette disposition d'être adoptée. Contrairement à ce qui a été dit, la disposition sur l'immunité pourrait avoir de vastes conséquences et poser grandement problème.

En particulier, elle vise à exploiter une partie de la confusion et de l'ambiguïté entourant la légalité de la divulgation de renseignements personnels aux autorités policières sans mandat. Elle vise également à profiter de l'ambiguïté de la législation actuelle en matière de protection de la vie privée et de l'évolution de ce qui constitue une attente raisonnable de protection de la vie privée dans le contexte des technologies de plus en plus avancées et envahissantes.

Par exemple, la loi actuelle pour le secteur privé en matière de protection de la vie privée, la Loi sur la protection des renseignements personnels et les documents électroniques, la LPRPDE, exige que les entreprises qui récoltent des renseignements personnels dans le cadre de leurs activités commerciales ne les divulguent pas sans que la personne le sache ou y consente. Il y a des exceptions importantes à cette règle, dont plusieurs sont rédigées de façon extrêmement générale et couvrent le fait de fournir des renseignements aux agences gouvernementales, y compris aux représentants des organismes d'application de la loi, dans une grande variété de circonstances. Il y a différentes interprétations de ce que permettent ces exceptions, et étant donné cette ambiguïté, les entreprises peuvent choisir d'adopter une approche plus prudente et qui protège la vie privée des clients par peur d'être poursuivies.

D'après nous, cette approche de prudence est appropriée, étant donné que les autorités policières ont l'expertise et la capacité nécessaire pour obtenir des mandats de perquisition. La disposition d'immunité est une tentative flagrante d'inciter les entreprises privées à coopérer avec des autorités policières, même si cela présente un réel risque à la protection de la vie privée des clients et ne servent pas un objectif clair de l'État. Cette disposition devrait être retirée du projet de loi.

Un certain nombre de nouveaux pouvoirs d'enquête sont inclus dans le projet de loi C-13 et permettent de préserver des données et de communiquer des documents selon le faible critère de « motifs raisonnables de soupçonner ». Ce critère est jugé approprié par nos tribunaux dans les contextes où les attentes raisonnables en matière de protection de la vie privée sont relativement faibles. Cependant, le projet de loi C-13 utilise ce critère pour autoriser des mandats pour la transmission de données et la localisation.

Contrairement à ceux qui disent que cela est comme les renseignements que l'on trouve dans l'annuaire téléphonique, ce n'est pas vrai. Ce genre de données peut vraiment porter atteinte à la vie privée d'une personne et fournir un profil détaillé et intime. De nombreuses données indiquent que dans certains cas, les renseignements que l'on peut obtenir à partir de ce genre de données sont plus importants que ce que l'on peut obtenir en surveillant le contenu des communications.

Je sais que je n'ai pas beaucoup de temps. Je veux souligner également certaines conséquences des changements à la définition de dispositif de localisation et d'enregistreur de transmission qui permettent l'installation de logiciels malveillants.

On donne le pouvoir aux policiers de pirater à distance des ordinateurs, des appareils mobiles ou des autos afin de localiser une personne et d'enregistrer des métadonnées. Dans certains cas, cela est fait en vertu du faible critère de « motifs raisonnables de soupçonner », qui d'après nous, est inapproprié.

Dans mon mémoire, j'ai présenté nos préoccupations en ce qui concerne le changement de définition de fonctionnaire public.

Enfin, je veux parler de nos préoccupations concernant l'absence de transparence et de mécanismes de reddition de comptes liés à certains des nouveaux pouvoirs créés par le projet de loi C-13.

● (1135)

Les nouveaux pouvoirs relatifs aux ordonnances de communication pourraient entraîner la divulgation de quantités importantes de renseignements personnels à la police et à bien d'autres organismes. Le projet de loi comprend une disposition qui prévoit, avec l'autorisation d'un juge, que l'existence de ces ordonnances sera tenue confidentielle pendant toute leur durée. Nous comprenons la nécessité de confidentialité pendant une enquête. Cependant, une fois que l'enquête est terminée, que l'intégrité de l'enquête n'exige plus que cette information soit tenue confidentielle, la personne visée devrait être informée du fait que ses données personnelles ont été divulguées.

Le président: Votre temps est écoulé, madame Zwibel.

Mme Cara Zwibel: Très bien, merci.

Le président: Vous pourrez peut-être nous en dire plus en réponse aux questions qui vous seront posées.

Mme Cara Zwibel: Merci.

Le président: Merci de votre exposé.

Notre prochain témoin représente Facebook. Madame Bickert, la parole est à vous.

Mme Monika Bickert (chef de la gestion des politiques, Facebook Inc.): Bonjour. Merci de m'avoir invitée.

Je m'appelle Monica Bickert. Je suis chef de la gestion des politiques globales chez Facebook. Je vais faire mon exposé en anglais.

Ma tâche à Facebook consiste à créer un environnement qui encourage les gens à s'exprimer et qui promeut la sécurité et le respect. Je me suis grandement investie pour faire en sorte que Facebook soit un endroit sûr où les gens se sentent à l'aise pour communiquer avec les personnes qui leur sont chères. Je ne dis pas cela seulement en tant qu'employée, mais en tant que mère de deux filles qui grandissent dans un monde de plus en plus branché.

Avant de travailler pour Facebook j'ai passé plus de 10 ans à lutter contre l'exploitation des enfants et la traite des personnes en tant que procureure fédérale aux États-Unis et comme conseillère juridique auprès de services de police étrangers. Je partage votre souci d'assurer la sécurité en ligne. C'est pourquoi je suis tellement fière de ce que nous faisons à Facebook pour donner aux gens la possibilité de se connecter et de partager d'une manière sûre et qui respecte leur vie privée.

Nous sommes au courant des questions complexes que le projet de loi C-13 soulève au sujet de la cyberintimidation, de l'application de la loi, de l'accès aux données et bien d'autres défis. Nous sommes heureux d'avoir l'occasion de vous faire part de notre point de vue sur notre approche en matière de sécurité et sur la façon dont les décideurs, les défenseurs de la sécurité et l'industrie peuvent travailler ensemble pour bâtir des collectivités plus sûres pour tous, en ligne et hors ligne. Nous croyons qu'il est important de comprendre les outils, les programmes et les partenariats que nous utilisons pour lutter contre le problème de la cyberintimidation.

La mission de Facebook est de contribuer à donner aux gens le pouvoir de partager et de rendre le monde plus ouvert et branché. Plus de 1,28 milliard de personnes du monde entier utilisent régulièrement Facebook pour partager de l'information — messages, photos, vidéos et mises à jour de leur statut — avec leurs amis et leur famille. Cela comprend plus de 19 millions de personnes ici au Canada. Facebook s'est engagé à conserver la confiance des personnes qui utilisent notre service et de leur fournir une expérience en ligne sécuritaire.

Nous avons élaboré une approche globale pour assurer la sécurité des enfants et des autres sur Facebook. Cela comprend l'application rigoureuse de nos normes communautaires, de robustes solutions et outils techniques et des partenariats avec des groupes qui se spécialisent dans la sécurité afin d'informer les gens sur les meilleurs moyens de se protéger et de protéger leurs amis et leur famille en ligne. Nous nous efforçons continuellement d'améliorer notre programme de sécurité et nous sommes heureux de recevoir les commentaires de nos utilisateurs, y compris des décideurs et des experts en matière de sécurité.

Nos normes communautaires indiquent clairement que nous avons un niveau de tolérance zéro pour l'intimidation, le harcèlement, les menaces et les contenus explicites comme la pornographie. Nous imposons des limites strictes en ce qui concerne la nudité. Nous tâchons de maintenir un juste équilibre entre le droit des gens de partager un contenu qui revêt pour eux une importance personnelle et la nécessité d'assurer un environnement sûr pour tous les membres de notre communauté. Nous avons des équipes dans le monde entier qui travaillent 24 heures sur 24, sept jours par semaine, pour répondre à des signalements de contenu qui pourraient enfreindre nos normes communautaires. Si le contenu ne respecte pas nos normes, nous le retirons du site. Nous pouvons également prendre d'autres mesures, comme donner des avertissements ou désactiver le compte de la personne qui a mis le contenu en ligne ou, dans des cas extrêmes, alerter la police au sujet de menaces de violence, d'actes autodestructeurs ou d'exploitation des enfants dans la vraie vie.

Nous donnons la priorité aux cas graves, ainsi qu'aux rapports de harcèlement, d'intimidation et d'autres formes d'abus, parce qu'il est très important pour nous que les gens se sentent en sécurité lorsqu'ils utilisent notre plateforme. Nous avons également déployé une technologie qui bloque le partage d'images d'exploitation d'enfants sur Facebook, y compris dans les groupes privés, ou qui les signale à l'attention immédiate de notre équipe de sécurité.

En collaboration avec Microsoft et le National Centre for Missing and Exploited Children aux États-Unis, nous utilisons une technologie qui s'appelle PhotoDNA (photo génétique). Cela nous permet d'identifier instantanément, d'éliminer et de signaler au centre national les images d'abus. Le centre national coordonne alors les mesures à prendre avec les polices étrangères.

● (1140)

Nous avons créé un conseil consultatif en matière de sécurité composé d'experts mondialement reconnus qui nous fournissent rapidement des conseils fondés sur l'expérience au sujet de nos produits et politiques. Nous essayons de faire en sorte que les gens puissent agir aussi facilement que possible pour régler les problèmes qu'ils ont ou qu'ils constatent lorsqu'ils sont sur Facebook. Non seulement nous avons des liens pour faciliter les rapports qui sont affichés bien en vue sur le site — ces liens se trouvent sur tous les éléments de contenu sur Facebook — nous avons aussi créé toute une gamme d'outils novateurs et de contrôles pour les adolescents, les parents et les éducateurs pour les aider à régler des conflits, en ligne et hors ligne. Par exemple, en nous fondant sur une recherche que nous avons faite pour déterminer de quelle manière les gens s'informent les uns les autres au sujet de problèmes, nous avons créé des outils de règlement des conflits sociaux novateurs afin d'aider les jeunes qui utilisent Facebook à demander de l'aide aux autorités, à leurs amis et aux membres de leur famille lorsqu'ils se trouvent dans une situation qui les rend mal à l'aise.

Nos outils de règlement de conflits sociaux aident également des jeunes à signaler les cas d'intimidation dont d'autres sont victimes et dont ils sont au courant. Comme la plupart des cas d'intimidation sur Facebook commencent et se terminent hors ligne, nous savons bien que malgré tous les efforts que nous faisons dans ce domaine, il reviendra toujours aux parents, aux enseignants et aux autres dirigeants communautaires qui sont les mieux placés pour comprendre ce qui se passe, d'intervenir lorsqu'il le faut.

Bien que ces outils soient importants pour aider les gens à agir dans leur propre intérêt et dans celui des autres, nous croyons également que nous avons un rôle important à jouer en informant les gens au sujet de nos politiques, sur la façon d'utiliser les outils pour s'aider et aider les autres et sur la façon d'avoir des conversations cruciales au sujet de la sécurité en ligne.

Cependant, nous ne pouvons pas agir seuls et c'est pourquoi nous avons créé des partenariats avec des organismes bien en vue qui rejoignent les jeunes de l'ensemble du Canada. Nous sommes fiers d'appuyer la campagne sur la cybersécurité du gouvernement du Canada. Nous avons travaillé avec des fonctionnaires, la Fédération canadienne des enseignantes et des enseignants pour promouvoir à l'échelle du pays notre guide « Réfléchissez avant de partager ». Ce guide qui est accessible au public donne aux jeunes les outils dont ils ont besoin pour partager d'une manière sécuritaire et responsable, ainsi que des conseils sur ce qu'ils devraient faire lorsqu'il y a un problème.

Le président: Vous permettez que je vous interrompe une seconde? Merci beaucoup.

Les cloches sonnent, mais les membres du comité s'étaient déjà entendus pour continuer après le début des cloches.

Il reste encore quelques minutes pour l'exposé en cours puis il y aura un autre exposé de 10 minutes. Je propose que nous écoutions les exposés, puis que nous allions voter et que nous revenions ensuite pour poser des questions.

Est-ce que cela convient à tous?

Des voix: D'accord.

Le président: Très bien.

Vous pouvez continuer, madame Bickert.

Mme Monika Bickert: Merci.

Encore une fois, je le répète, nous ne pouvons pas agir seuls.

Au Canada, pendant la Semaine de la sensibilisation à l'intimidation, nous avons travaillé en partenariat avec sept organismes canadiens qui prêchent la sécurité, y compris PREVNet, Jeunesse, J'écoute et HabiloMédias dans le cadre de la campagne « Osez. Dites non au harcèlement ». Les étudiants de tout le pays ont appris ce qu'ils peuvent faire pour mettre fin à l'intimidation et se sont engagés à empêcher l'intimidation dans leur collectivité.

Nous sommes heureux que le gouvernement souhaite moderniser les outils dont dispose la police pour lutter contre l'intimidation et le harcèlement et nous sommes d'accord pour trouver des moyens de lui donner les outils dont elle a besoin pour lutter contre la cybercriminalité dans le respect de la vie privée des Canadiens. En tant qu'industrie, nous avons demandé aux gouvernements de veiller à ce que tous les efforts de la police pour collecter des données soient conformes avec les normes internationales en matière de liberté d'expression et de protection de la vie privée, ce qui veut dire que cette collecte doit être régie par des règles et des restrictions strictement adaptées, doit être transparente et faire l'objet d'une supervision. Nous croyons que ces principes sont fondamentaux pour la protection de la vie privée.

En terminant, j'aimerais remercier à nouveau le comité de m'avoir donné l'occasion de m'adresser à vous aujourd'hui. Nous tous à Facebook avons comme vous à coeur d'assurer la sécurité des Canadiens en ligne. Je suis heureuse d'avoir eu l'occasion de vous faire part des mesures que nous prenons pour maintenir une communauté sécuritaire et de vous avoir fait part de nos idées pour créer un meilleur Internet.

C'est avec plaisir que je répondrai à vos questions après la pause.

● (1145)

Le président: Merci beaucoup, madame Bickert, de votre exposé.

Notre prochain témoin comparaîtra par vidéoconférence, à partir de Washington D.C. Souhaitons la bienvenue à M. Beckerman, président de l'Internet Association.

J'espère que vous pouvez m'entendre. La parole est à vous pendant 10 minutes.

M. Michael Beckerman (président, The Internet Association): Merci. Veuillez m'excuser de ne pas pouvoir me présenter à vous en personne.

Je m'appelle Michael Beckerman et je suis le président de l'Internet Association, une organisation qui représente 25 des principales sociétés Internet du monde. Nos membres sont des chefs de file dans l'industrie d'Internet et, à titre d'industrie, ils s'engagent à fournir des services de premier ordre afin d'aider à améliorer le monde. L'Internet Association est ravie de pouvoir vous parler du projet de loi C-13, visant à protéger les Canadiens du crime en ligne.

L'intimidation menace la capacité qu'ont les gens de communiquer de manière sécuritaire et confidentielle. Elle peut avoir des conséquences considérables auprès des gens concernés. Les conséquences sont exactement les mêmes, que l'intimidation ait lieu dans les salles de classe, sur un terrain de jeu ou sur un site Web. Il ne s'agit pas d'un problème qui touche un site Web, une école ou un médium en particulier.

Il est évident qu'aucune personne dans notre société ne peut à elle seule régler ce problème sempiternel. Il s'agit plutôt d'un problème sur lequel tous les intervenants — les familles, les amis, les enseignants, les leaders dans la collectivité, les gouvernements et le secteur privé — devraient se pencher collectivement.

Pour sa part, l'industrie d'Internet a travaillé de manière proactive pour répondre aux préoccupations en ce qui a trait à l'intimidation qui survient en ligne, notamment, par le biais de campagnes de sensibilisation, d'efforts pour prévenir le suicide et de solutions techniques robustes pour répondre au problème de l'intimidation lorsqu'il survient.

Plusieurs sociétés d'Internet, dont Google, Twitter, Facebook et Yahoo ont collaboré avec un organisme à but non lucratif intitulé SAVE afin de mettre sur pied le guide *Responding to a Cry for Help: Best Practices for Online Technologies*. Il s'agit d'un guide dans lequel des entreprises Internet et des sociétés en démarrage partagent les pratiques exemplaires des sociétés de haute technologie les plus en vue pour réduire le risque de suicide chez les utilisateurs.

De plus, nos membres travaillent de près avec des groupes tels le Centre canadien de protection de l'enfance, HabiloMédias et d'autres, pour élaborer des campagnes de sensibilisation publiques ciblées qui portent sur l'alphabétisation numérique, [*Inaudible: note de l'éditeur*] les habitudes en ligne et les ressources pour lutter contre l'intimidation. Ces efforts sont essentiels pour mettre un terme à l'intimidation avant même qu'elle ne commence.

Plusieurs de nos membres ont également créé un partenariat avec la Family Online Safety Institute, qui représente une organisation mondiale. Ils appuient leur « A Platform for Good », une plateforme conçue pour aider les parents, les enseignants et les adolescents à entrer en contact les uns avec les autres, à partager leur expérience et à faire de bonnes choses en ligne, afin d'améliorer la sécurité en ligne pour tous.

En ce qui a trait aux outils innovateurs en ligne, nos membres ont des mécanismes rigoureux pour signaler les abus, avec, notamment, le recours à des boutons de signalement d'abus qui sont faciles à utiliser et des liens qui sont liés à un contenu généré par l'utilisateur. Nos sociétés ont également des systèmes automatisés, ainsi que des équipes de personnes qui se retrouvent partout dans le monde et qui examinent, enlèvent immédiatement et répondent à un contenu qui va à l'encontre des modalités de service très rigoureuses et aux lignes directrices de notre collectivité.

Bien qu'il n'y ait pas de solution unique pour répondre au problème de l'intimidation en ligne et hors ligne, nous sommes fiers du leadership dont font preuve nos membres lorsqu'ils apportent de nouvelles idées, des nouvelles ressources et de nouvelles technologies afin d'aider notre collectivité à faire des progrès dans cet important dossier.

Les membres de l'Internet Association comprennent que, afin de continuer à avoir une société sécuritaire, on a besoin de faire appel aux organismes d'application de la loi. Nos membres appuient la mission importante des forces de l'ordre qui veillent à préserver la sécurité des gens. En même temps, nous reconnaissons le fait que les gens choisissent d'utiliser des services Internet pour entreposer leurs renseignements les plus confidentiels et personnels. À cette fin, nous estimons que les forces de l'ordre devraient être assujetties à un seuil accru, telles que l'obligation d'obtenir un mandat judiciaire fondé sur des critères appropriés afin de pouvoir avoir accès au contenu des utilisateurs, que cela survienne dans l'espace cybernétique ou physique.

Nos membres s'engagent à respecter leurs obligations en ce qui a trait à travailler avec les enquêtes criminelles légitimes et vont même plus loin en créant des relations positives avec les forces de l'ordre, et en travaillant de près avec elles dans des circonstances appropriées. Nous ne croyons pas que la promotion de la sécurité du public exige que le gouvernement réduise le seuil juridique nécessaire pour avoir accès aux communications privées des gens. En effet, la confiance du public fait en sorte que nous nous tenons et nous tenons nos responsables aux normes les plus élevées dans ce domaine fort important.

Un des outils les plus importants utilisés par nos membres pour obtenir la confiance du public est la transparence. Plusieurs de nos membres publient le nombre et le genre d'enquêtes qu'ils reçoivent des gouvernements partout dans le monde. Nous continuons à croire que le gouvernement devrait être le plus transparent possible en ce qui a trait aux demandes qu'ils font auprès de sociétés telles que Google, Twitter, Facebook et d'autres. Les sociétés devraient avoir le droit de dire aux gens lorsque leurs renseignements sont recueillis par le gouvernement, et leur dire individuellement lorsque les circonstances le permettent et sinon leur fournir des données globales.

Nous craignons que le libellé du projet de loi C-13 nous mène dans la direction opposée. Plus précisément, le paragraphe 487.019 (1) permettrait à un juge d'interdire aux gens de divulguer l'existence d'une partie ou de tout le contenu d'une ordonnance de préservation ou de communication et des renseignements personnels d'une personne.

● (1150)

Bien que nous reconnaissons le fait que, dans certains cas, ce genre de divulgation pourrait mettre en péril la sécurité du public, cette disposition du projet de loi C-13 pourrait permettre au gouvernement d'interdire aux sociétés de divulguer l'existence même de telles ordonnances d'obtention de données de la part des gouvernements, y compris le nombre des demandes et la communication éventuelle d'information.

Nos membres publient ces genres de renseignements, car ils estiment que les gens devraient avoir le droit de comprendre la nature et la portée des renseignements que le gouvernement veut obtenir à leur endroit. Ces rapports donnent plus de confiance aux gens en leur gouvernement, et leur permet de voir qu'ils agissent d'une manière appropriée et restreinte, lorsqu'ils demandent d'obtenir des renseignements au sujet des utilisateurs. Cela permet également aux gens de se sentir à l'aise lorsqu'ils s'expriment en ligne.

Nous exhortons le comité à envisager de modifier ce libellé ainsi que toute autre tentative de bâillonnement dans le projet de loi C-13 afin de pouvoir, à tout le moins, permettre expressément aux sociétés de rapporter le nombre global d'ordonnances de préservations et de communications qu'elles ont reçues. En continuant à interdire la divulgation du contenu de ces ordonnances dans les cas très restreints où le contenu d'une ordonnance est particulièrement délicat pour des raisons de sécurité, on pourra permettre la transparence sans pour autant mettre en péril la sécurité du public ou nuire aux enquêtes légitimes.

Comme d'autres l'ont mentionné publiquement, le projet de loi semble fournir au gouvernement des pouvoirs qui font en sorte qu'il n'a pas besoin de mandat pour obtenir des données ou encore qu'il puisse obtenir un mandat selon des critères inférieurs à ceux que l'on applique à l'heure actuelle dans le monde hors ligne.

J'aimerais notamment mettre l'accent sur ce dernier point.

Sauf tout le respect que je vous dois, j'exhorte le comité à se demander s'il est véritablement opportun d'abaisser le seuil juridique nécessaire pour obtenir un mandat afin que le gouvernement puisse avoir accès au contenu des utilisateurs. C'est ce que l'on propose dans le projet de loi C-13. D'après notre compréhension du projet de loi, les forces de l'ordre n'auraient qu'à démontrer à un juge qu'ils ont des motifs raisonnables de soupçonner que quelqu'un a commis un crime ou commettra un crime afin de pouvoir obtenir le mandat en question. En vertu de la loi actuelle, les agents de la paix doivent se conformer à un seuil juridique plus élevé dans lequel ils doivent prouver qu'ils ont des motifs raisonnables de croire qu'un crime a été commis avant de pouvoir obtenir un tel mandat.

De plus, la législation semble permettre aux juges de tenir compte d'un seuil juridique plus faible lorsqu'ils déterminent que les preuves provenant d'une fouille légitime fourniront des preuves en ce qui a trait à la perpétration d'une infraction. À la place, ils pourraient octroyer des mandats pour le simple motif qu'ils sont utiles à l'enquête. Cela est perçu par bon nombre de gens comme un seuil juridique bien inférieur.

En ce qui a trait à la question délicate des renseignements personnels, surtout dans les circonstances où les gens ne savent pas qu'ils sont sous enquête, il est important que nous envoyions un message clair aux gens pour qu'ils comprennent que ce genre d'enquêtes n'auront lieu que dans des cas très restreints et dans lesquels on respectera un seuil juridique très élevé.

L'Internet Association craint que le fait d'abaisser le seuil juridique, tel que le propose le projet de loi, compromettra les renseignements personnels des gens qui utilisent Internet et réduira la confiance qu'ont les citoyens que le gouvernement respecte leurs droits à un procès juste et équitable. À la lumière de ces préoccupations, nous exhortons le comité à revenir aux normes de protection des renseignements qui existent à l'heure actuelle dans le Code criminel.

Nos membres représentent des sociétés responsables qui s'engagent à garantir la sécurité des citoyens canadiens en ligne. L'industrie d'Internet continuera à innover et à créer des technologies et des outils de fine pointe et à travailler sur des programmes et des partenariats pour lutter contre la cyberintimidation et l'intimidation en général.

Nous apprécions que le comité porte attention à cet enjeu fort important que soulève le projet de loi C-13. Nous sommes heureux d'avoir eu l'occasion de vous présenter nos points de vue et j'ai hâte de répondre à vos questions.

Merci.

● (1155)

Le président: Merci, monsieur Beckerman.

Nous allons maintenant suspendre la séance.

J'aimerais vous dire que, selon l'heure à laquelle nous arriverons là-bas, j'aimerais reprendre la séance à 12 h 30. Si on peut s'organiser pour reprendre à 12 h 30, ce serait idéal. Nous aurions alors une série de questions, la première série, soit sept minutes. Nous aurions donc une première série de questions de sept minutes et ce serait tout le temps disponible pour les questions.

Merci beaucoup.

Nous allons suspendre la séance et apprécions votre patience pendant que nous allons voter.

● (1155)

_____ (Pause) _____

● (1235)

Le président: Je déclare la séance à nouveau ouverte.

Laissez-moi présenter à nouveau nos excuses à nos témoins et les remercier de leur patience.

Nous sommes revenus du vote et ne serons plus interrompus. Nous allons faire une série de questions, je crois, de sept minutes environ pour chaque personne, comme je l'ai indiqué auparavant.

La première série de questions est pour le Nouveau Parti démocratique avec Mme Boivin.

[*Français*]

Mme Françoise Boivin (Gatineau, NPD): Merci aux témoins.

[*Traduction*]

Merci beaucoup. Au cas où je passerais d'une langue à l'autre, soyez prêt à vous prévaloir des services d'interprétation.

Je vous remercie de votre témoignage, notamment M. Kempton. Je suis désolée de ce qui s'est produit. Votre récit m'a touchée. Il va nous falloir trouver un équilibre approprié, sans perdre de vue le vrai monde qui est affecté par les projets de loi auxquels nous travaillons. C'est une promesse que je vous fais.

[*Français*]

C'est la même chose pour vous, monsieur Wamback.

[*Traduction*]

Merci beaucoup de votre témoignage.

Il est rare qu'on puisse entendre Facebook et l'Internet Association.

C'est à Facebook en quelque sorte que je vais poser mes questions, parce que j'ai entendu votre témoignage au nom de Facebook. Je suis une adepte de Facebook, si bien que je ne voudrais pas que vous preniez mal mes remarques. Je figure parmi vos 18 ou 19 millions de membres au Canada.

Ceci dit, je me souviens de ce qui s'est passé l'an dernier, quand quelqu'un a essayé d'usurper mon identité. C'était comme de se réveiller un matin et d'avoir des gens qui disaient: « Je ne crois pas que ce soit toi. » Cela a été retiré sans problème, mais nous avons entendu des témoignages indiquant que ce n'est pas toujours le cas.

Vous avez beaucoup parlé des efforts et des choses que fait Facebook.

Par contre, vous n'avez pas beaucoup parlé du projet de loi. J'aimerais donc savoir ce que Facebook pense du projet de loi C-13: ce qui vous plaît, ainsi que les éléments, s'il y en a, qui, selon vous, mériteraient d'être retravaillés. Je pense qu'on a eu une bonne explication de ce que Facebook fait pour améliorer la sécurité, etc., mais comment est-ce que cela s'applique au projet de loi C-13? Facebook est-il préoccupé par le projet de loi C-13? Pensez-vous que les ordonnances des tribunaux pourraient s'appliquer?

La question pourrait également s'adresser à M. Beckerman, vu qu'une bonne part d'entre vous n'ont pas leur siège au Canada.

Comment est-ce que cela va affecter les sociétés que vous représentez, juridiquement, monsieur Beckerman ou Facebook?

Madame Bickert, êtes-vous préoccupée par le projet de loi C-13? Vous n'avez rien dit à ce sujet.

M. Michael Beckerman: Je serais heureux de commencer.

Le président: Nous allons commencer par Mme Bickert, après quoi ce sera votre tour.

M. Michael Beckerman: D'accord alors tout d'abord...

Le président: Monsieur Beckerman, nous commençons par Mme Bickert. Merci.

Mme Monika Bickert: Merci.

Nous sommes une société véritablement internationale et avons adopté une série de politiques qui s'appliquent en fait aux utilisateurs de Facebook où qu'ils soient dans le monde. Ceci dit, nous respectons bien sûr toutes les lois qui s'appliquent à nous. Mais vu notre caractère international, nous adoptons une approche vraiment générale en réfléchissant à ces questions.

Dans mon témoignage, j'ai présenté certaines de nos approches conceptuelles. Quand il s'agit de protéger les gens, nous voulons avoir une politique bien définie. Nous voulons qu'il soit facile pour les gens de rapporter certaines choses et j'espère que le processus a été facile pour vous quand vous vous êtes heurtée à un problème dans Facebook. Je peux vous dire que si on nous signale un contenu qui constitue une intimidation ou du harcèlement, nous réagissons rapidement et enlevons ce contenu.

Mme Françoise Boivin: Avez-vous entendu le témoignage de M. Canning, le père de Rehtaeh Parsons, l'une des jeunes qui, hélas, se sont suicidés? Il a dit que c'était difficile, qu'on lui avait dit que cela n'allait pas à l'encontre des règles de la communauté de Facebook. Il y avait certaines images où on voyait la jeune en train de... Elle est morte.

● (1240)

[*Français*]

Elle s'était pendue. Je ne sais pas comment le dire en anglais.

[*Traduction*]

Elle s'est pendue ou quelque chose dans ce genre. Il y avait des images assez horribles. Alors quand j'entends quelqu'un de votre groupe répondre que cela n'allait pas à l'encontre des règles de la communauté de Facebook, qu'avez-vous à dire?

Mme Monika Bickert: Je ne peux pas bien sûr parler de ce cas particulier mais, ce type de contenu, où quelqu'un met en scène un suicide, va indubitablement à l'encontre de nos normes et serait enlevé. C'est une priorité pour nous, au point où nous accordons un statut prioritaire à tout rapport d'intimidation ou de harcèlement, afin d'y réagir très rapidement, n'importe où dans le monde.

Quant à votre autre remarque, je ne sais pas s'il est plus approprié...

Le président: Je vais lui demander de répondre.

Monsieur Beckerman, à vous la parole.

M. Michael Beckerman: Merci. Je regrette, il y avait un certain retard, avant.

Pour revenir à votre remarque sur la façon dont les sociétés membres de notre association réagissent aux citoyens canadiens ou ont un siège aux États-Unis, je dirais que les sociétés membres de notre association sont internationales et qu'elles estiment représenter les communautés d'utilisateurs qu'elles desservent, tant au Canada que partout dans le monde.

Dans ces domaines, il y a eu un certain nombre de cas profondément attristants, des cas horribles, ce que nos sociétés prennent vraiment au sérieux. Elles accordent une forte priorité à la sûreté et la sécurité des utilisateurs tant au Canada que partout dans le monde.

Je pense que vous devriez considérer notre secteur dans son ensemble, et plus particulièrement les sociétés membres de notre association, qui sont toutes de bons agents dans ce domaine et travaillent en collaboration avec les autorités au Canada et avec des groupes d'enseignants, afin d'éduquer les élèves et étudiants au Canada. Il serait bon de ne pas nous voir comme un problème, mais comme partie prenante de la réponse à y apporter.

Mme Françoise Boivin: Avez-vous été approchés par une force de police quelconque qui vous demandait de divulguer des renseignements? Peut-être est-ce le cas d'une de vos sociétés, de Facebook, peut-être? Avez-vous été approchés par les autorités pour certains cas au Canada? Vous a-t-on demandé de divulguer certains renseignements et, si oui, en avez-vous informé les personnes concernées?

Le président: Nous allons commencer par M. Beckerman concernant les demandes de la police et nous finirons par Facebook. Merci beaucoup.

M. Michael Beckerman: Je ne peux pas entrer dans le détail d'exemples de sociétés particulières et de cas particuliers. Ce que je peux affirmer, c'est que toutes les sociétés membres de notre association travaillent avec les collectivités locales et les forces de maintien de l'ordre locales. Elles consacrent notamment beaucoup de temps et de ressources aux cas qui mettent en danger la sécurité ou la vie de certaines personnes. C'est un élément très important pour nos sociétés.

La qualité d'une plateforme dépend entièrement de ce qu'en font les gens et de la sécurité en ligne, si bien qu'il est très important que nous travaillions avec les forces de maintien de l'ordre dans ces cas.

Le président: Je vais laisser Mme Bickert répondre.

Mme Monika Bickert: Chaque fois que nous recevons une demande de renseignements provenant d'un gouvernement quelconque, nous avons un processus permettant de l'examiner en fonction de nos termes et des lois applicables et nous fournissons des renseignements quand c'est stipulé par la loi.

Nous sommes convaincus de l'importance de la transparence. Il faut que les utilisateurs de Facebook sachent comment nous protégeons leurs données et quand nous sommes susceptibles de les fournir à des agences de maintien de l'ordre. C'est pourquoi c'est indiqué très clairement dans nos termes. Nous avons une politique d'utilisation des données précisant comment nous sommes susceptibles de répondre et comment nous examinons les demandes de la part d'agences de maintien de l'ordre. Nous allons plus loin, dans la mesure où nous avons rendu publics des renseignements dans une série de rapports sur des demandes du gouvernement où nous disons aux gens quelles sont les demandes que nous recevons partout dans le monde et comment nous y répondons.

Mme Françoise Boivin: Pour la clause d'immunité, est-ce important pour vos sociétés? Et quel type d'immunité recherchez-vous?

Le président: C'est la dernière question.

Madame Bickert.

Mme Monika Bickert: Nous avons établi clairement dans notre politique sur l'utilisation des données les circonstances dans lesquelles nous pouvons fournir de l'information à un gouvernement. Il s'agit essentiellement d'une situation où nous recevrions une demande provenant d'un gouvernement, et nous appliquerions un examen rigoureux à cette demande pour nous assurer qu'elle n'est pas trop générale et faire en sorte qu'elle est conforme à la loi.

Dans de rares cas, qui sont très clairs dans nos conditions, parce que nous avons le souci de protéger les gens, nous indiquons que si nous croyons que la vie d'une personne est en danger ou qu'elle pourrait subir des préjudices physiques, à ce moment-là nous fournirons l'information aux responsables de l'application de la loi au besoin pour protéger les gens.

● (1245)

Le président: Monsieur Beckerman, voulez-vous réagir à cette question?

M. Michael Beckerman: Je suis d'accord avec ce qui a été dit. Du point de vue de la transparence, nos sociétés membres se font toutes un point d'honneur de publier ces rapports sur la transparence. Il est important que les gens comprennent le type de renseignements qui est recueilli par le gouvernement et que cela réponde à leurs besoins et à leurs craintes en matière de protection de la vie privée.

Le président: Merci pour ces questions et ces réponses.

Notre prochain intervenant est M. Dechert, du Parti conservateur.

M. Bob Dechert (Mississauga—Erindale, PCC): Merci, monsieur le président et merci à chacun de nos invités de se joindre à nous aujourd'hui.

Monsieur Kempton, je veux joindre ma voix à celle de Mme Boivin et exprimer mes condoléances à vous et à votre famille pour les terribles événements qui sont arrivés à votre petite-fille.

Je peux vous assurer que votre présence aujourd'hui et tout le travail que vous avez fait précédemment, y compris les nombreuses allocutions publiques que je sais que vous avez prononcées, et les bourses dont vous avez parlé changeront les choses pour les jeunes. Nous sommes d'accord avec vous, l'éducation est tout à fait primordiale dans ce cas-ci.

Nous examinons un projet de loi qui mettra en place des dispositions au Code criminel nous permettant de lutter contre les exemples les plus flagrants de cyberintimidation et de donner aux autorités les outils d'application de la loi dont ils ont besoin pour faire enquête. Mais, le plus important, c'est de faire comprendre à tous le pouvoir et la vitesse d'Internet et des médias sociaux afin qu'ils puissent prendre les mesures nécessaires pour se protéger et empêcher que des choses comme celles-là ne se produisent.

Je vous remercie donc d'être présent et j'apprécie vos observations.

Monsieur Wamback, je suis heureux de vous revoir. Je sais que vous avez déjà témoigné de nombreuses fois devant notre comité, et vous devenez tout un expert en matière de droit criminel. Je vous en remercie.

J'ai été frappé par quelque chose que vous avez dit et cela ressemblait à ce que nous avons entendu de la part de Glen Canning, le père de Rehtaeh Parsons. Vous avez dit que l'anonymat n'existe pas sur Internet.

Pouvez-vous préciser ce que vous entendez par là?

M. Joseph Wamback: Selon mon expérience, non seulement personnelle mais aussi celle d'autres Canadiens, lorsqu'ils font l'objet d'intimidation, que leurs vies sont menacées et que de fausses rumeurs sont répandues à leur sujet dans divers médias, et non pas seulement les médias sociaux, mais dans différents blogues et courriels individuels, cela a lieu et est facilité en raison de l'anonymat qui existe à l'heure actuelle. Quiconque peut se connecter dans un site de médias sociaux en utilisant n'importe quel nom et justificatif de l'identité pour se créer une identité et continuer de s'en servir.

La seule chose qui est à la disposition des policiers et des autorités pour identifier cette personne, c'est l'adresse URL, l'emplacement et l'identité de l'ordinateur.

Cela rend les choses à l'heure actuelle difficiles, voire impossibles. Pendant cinq ans, j'ai essayé de retracer les individus qui ont entaché la réputation de ma famille et proféré des menaces de mort à notre égard, et chaque fois, je me suis fait dire que c'était peine perdue, que c'était impossible et que cela ne pouvait pas se faire.

Ce que je souhaite relativement à ce projet de loi, c'est que, dans ce genre de circonstances, nous puissions être en mesure d'exiger des comptes de la part de ceux qui utilisent ces médias pour intimider les gens et faire des menaces, et j'aimerais qu'il y ait des conséquences associées à ces gestes.

M. Bob Dechert: M. Canning a rappelé qu'en adhérant à des sites comme Facebook ou d'autres sites de médias sociaux, les gens fournissent quantité de renseignements personnels. Ces organisations s'en servent à diverses fins. Parfois c'est à des fins publicitaires, comme Google ou d'autres systèmes, mais les seules personnes qui n'ont pas ces renseignements sont les autorités qui tentent d'enquêter sur un crime potentiel.

Madame Bickert, vous m'avez dit que les abonnés à Facebook doivent fournir leur véritable nom et que vous prenez les mesures nécessaires pour faire une vérification à cet égard. Pouvez-vous nous en dire davantage là-dessus?

Mme Monika Bickert: Volontiers.

Facebook exige que nos abonnés utilisent leur véritable identité. Nous pensons que cela aide les gens à se retrouver car un nom est essentiel à l'identité. Par ailleurs, nous constatons que cela permet une plus grande reddition de comptes.

Nous avons fait de notre mieux pour affirmer clairement dans nos consignes que le nom est exigé — si bien qu'on s'y attend — et nous avons les moyens grâce à des rapports de savoir si quelque chose ne va pas ou si quelqu'un n'utilise pas son véritable nom. Dans de tels cas, nous faisons enquête sur le profil et s'il s'avère que c'est une fausse identité, nous supprimons ce profil.

● (1250)

M. Bob Dechert: Merci de cette réponse.

Je tiens à signaler que Facebook fait un excellent travail à cet égard et a recours à d'autres outils pour empêcher l'intimidation et supprimer de façon proactive tout contenu douteux. À cet égard, Facebook fait preuve de bonne conscience sociale. Je vous en suis reconnaissant.

Mme Monika Bickert: Merci.

M. Bob Dechert: Monsieur Wamback, vous avez fait allusion à la Loi sur le système de justice pénale des adolescents. Je peux vous garantir qu'aucune disposition du projet de loi C-13 n'empêche l'application de cette loi.

M. Joseph Wamback: Merci.

Mon souci était l'absence de renvoi. Je suis un peu chatouilleux à cet égard, mais mon argument était strictement d'ordre administratif. Je voulais m'assurer que ces dispositions n'empêchent pas l'application de tous les autres articles du Code criminel.

M. Bob Dechert: Nous pensons que c'est le cas, mais nous pouvons certainement fouiller la question.

M. Joseph Wamback: Merci.

M. Bob Dechert: Madame Zwibel, avez-vous pris connaissance du rapport du groupe de travail sur la cybercriminalité, lequel était composé de représentants des procureurs généraux de chaque province et territoire?

Mme Cara Zwibel: Oui.

M. Bob Dechert: Et vous connaissez les recommandations qui figurent dans le rapport, n'est-ce pas?

Mme Cara Zwibel: Oui.

M. Bob Dechert: Y a-t-il certaines recommandations que vous désapprouvez?

Mme Cara Zwibel: Je les ai lues, il y a un certain temps et je sais qu'une des recommandations a abouti à cette proposition de créer une nouvelle infraction, à savoir la distribution non consensuelle d'images intimes. Comme je l'ai dit tout à l'heure, ce n'est pas le fait qu'on crée une infraction qui nous pose problème, mais son libellé.

Les recommandations du rapport préconisaient un accroissement des pouvoirs d'enquête, dont traite d'ailleurs le projet de loi...

M. Bob Dechert: Approuvez-vous ces recommandations?

Mme Cara Zwibel: Non. Dans mon exposé, j'ai exprimé mon désaccord à l'égard de certaines d'entre elles. Ce qui nous inquiète, c'est ce qui constitue un motif raisonnable de soupçonner pour...

M. Bob Dechert: Autrement dit, votre organisation désapprouve les recommandations que le groupe de travail sur la cybercriminalité a faites à cet égard?

Mme Cara Zwibel: Oui, c'est exact.

M. Bob Dechert: Merci.

Vous avez fait allusion à une prétendue disposition sur l'immunité, au paragraphe 487.0195. Connaissez-vous l'article 25 du Code criminel?

Mme Cara Zwibel: Oui.

M. Bob Dechert: Il prévoit certaines mesures de protection pour ceux qui coopèrent avec les forces de l'ordre.

Mme Cara Zwibel: En effet. Le libellé de l'article 25... Je sais que cela a été soulevé à d'autres...

M. Bob Dechert: Puis-je vous poser une autre question? Je crois qu'elle est pertinente.

Mme Cara Zwibel: Certainement.

M. Bob Dechert: Connaissez-vous l'affaire *R.* c. *Ward* et la décision du juge Doherty de la Cour d'appel de l'Ontario?

Mme Cara Zwibel: Oui, je connais l'affaire dont vous parlez.

M. Bob Dechert: Pris ensemble, l'article 25 et cette décision du juge Doherty de la Cour d'appel de l'Ontario, ne croyez-vous pas que cela donne une certaine immunité aux fournisseurs de services Internet et aux autres à qui les policiers demandent de fournir volontairement des renseignements de base sur leurs abonnés, tels que le nom et l'adresse?

Mme Cara Zwibel: Ma réponse, c'est que cela dépend. Les renseignements de base sur les abonnés qui seraient donnés en échange, par exemple, des numéros de téléphone inscrits et le genre de renseignements que l'on s'attend à trouver dans un annuaire téléphonique et que l'on sait qu'ils sont généralement disponibles publiquement. Lorsqu'il y a une demande des policiers auprès d'un fournisseur de services Internet, d'une entreprise de télécommunications, et que la base de la demande est une adresse IP, une adresse de protocole Internet, c'est une demande de renseignements sur les abonnés. D'après moi, cela révèle plus que ce qui est disponible publiquement. Cela révèle où vous allez sur Internet, les sites que vous visitez.

M. Bob Dechert: Mais pas le contenu, les images ou d'autres choses comme ça.

Mme Cara Zwibel: Pas les contenus ou les images, mais si vous connaissez le site qu'une personne visite, vous pouvez trouver ce que ce site contient.

M. Bob Dechert: Merci.

Madame Bickert, pourrais-je vous demander ce que vous pensez que divulgue une adresse IP? Si Facebook demande ce renseignement, que croyez-vous que vous divulguez aux policiers?

Mme Monika Bickert: Lorsque nous fournissons...?

M. Bob Dechert: Les renseignements sur un abonné à partir d'une adresse IP, par exemple.

Mme Monika Bickert: Nous fournissons des renseignements qui ne sont pas du contenu, telles que des adresses IP, lorsque nous recevons des demandes à motif juridiquement suffisant du gouvernement. À part cela, je ne suis pas certaine de pouvoir...

M. Bob Dechert: C'est couvert par votre accord et les politiques qu'acceptent les gens lorsqu'ils s'inscrivent à Facebook?

Mme Monika Bickert: Absolument, tout est très transparent.

M. Bob Dechert: D'après vous, que divulgue une adresse IP? Est-ce seulement le nom et l'adresse de la personne qui envoie les données, ou d'autres choses?

Mme Monika Bickert: Nous fournissons l'adresse IP. Comment elle est utilisée ou...

M. Bob Dechert: Est-ce qu'ils iraient ensuite à l'adresse IP?

Mme Monika Bickert: Je ne le sais pas.

Le président: Pas de problème. Merci beaucoup pour ces questions et ces réponses.

Les dernières questions viendront de M. Casey du Parti libéral.

● (1255)

M. Sean Casey (Charlottetown, Lib.): Merci, monsieur le président.

Madame Zwibel, on vous a posé une question sur le lien entre l'article 25 du Code criminel et le projet de loi C-13. Vous avez commencé à feuilleter vos documents pour trouver une réponse, mais on ne vous a pas donné le temps de la présenter. Vous en avez maintenant l'occasion.

Mme Cara Zwibel: Merci.

L'article 25 indique que si vous faites ce qui vous est enjoint ou permis de faire par la loi, et que vous vous appuyez sur des motifs raisonnables, vous êtes justifié de le faire. C'est en gros une justification pour la défense. C'est un peu différent de l'immunité globale au civil et au criminel proposée par le projet de loi C-13. La disposition du projet de loi C-13 n'exige pas de motifs raisonnables, alors je crois que c'est une distinction importante. Dans ce sens, je crois que de parler de l'article 25 est un peu une diversion.

M. Sean Casey: Je le crois également. Merci.

Monsieur Beckerman, à votre connaissance, est-ce que votre association ou certains de ses membres ont été consultés dans le cadre de la rédaction de ce projet de loi?

M. Michael Beckerman: À ma connaissance, l'association n'a pas été consultée. Je ne peux pas dire s'il y a des entreprises qui ont été consultées à ce sujet.

M. Sean Casey: Est-ce que l'immunité contre des poursuites au civil et au criminel pour la divulgation volontaire de renseignements aux autorités policières au Canada est quelque chose que votre association ou certains de ses membres demandaient?

M. Michael Beckerman: Comme je l'ai dit, je ne connais pas les discussions que chacune de nos entreprises peut avoir eu avec le comité qui a rédigé le projet de loi. À ma connaissance, l'association n'a pas participé à sa préparation.

M. Sean Casey: Est-ce que des entreprises de télécommunications sont membres de votre association?

M. Michael Beckerman: Non.

M. Sean Casey: La prochaine question s'adresse à Mme Bickert et aussi à M. Beckerman.

Vous avez tous les deux parlé de rapports sur la transparence. Je ne sais pas si vous savez qu'il est très difficile d'obtenir le genre de renseignements que vous divulguez volontairement de la part des entreprises de télécommunications. Je parle de la distribution non consensuelle des renseignements sur les clients, sans mandat.

Qu'est-ce que les entreprises de télécommunications, et peut-être le gouvernement, peuvent apprendre de vos pratiques en matière de rapport sur la transparence?

Le président: Madame Bickert, voulez-vous répondre la première?

Mme Monika Bickert: La confiance est la pierre angulaire de nos activités. La réalité est que si les gens ne font pas confiance à Facebook, ils ne l'utiliseront pas. Pour cette raison, nous disons clairement, en vertu de nos politiques et de nos pratiques, que la transparence est primordiale pour nous. C'est pourquoi nous avons mis en place ces procédures. Cela comprend non seulement la description de la protection des données et comment elles peuvent être fournies à la suite d'une demande légale de la part du gouvernement, mais aussi la préparation de rapports volontaires sur la transparence afin que les gens comprennent l'ampleur dans laquelle le gouvernement veut avoir accès aux données.

Le président: Monsieur Beckerman.

M. Michael Beckerman: Merci.

Je ne peux pas parler pour les fournisseurs de télécommunications. Mais dans notre industrie, la transparence et la confiance des utilisateurs sont primordiales. Nos sites ne sont bons que dans la mesure où les utilisateurs les utilisent. Dans notre secteur, la concurrence est partout et n'est qu'à un clic sur Internet, ce dont nous sommes très conscients. Alors la transparence et la reddition de comptes aux utilisateurs sont extrêmement importantes et primordiales pour l'industrie.

M. Sean Casey: Si le gouvernement était d'accord avec vous, il n'y a aucune raison qui l'empêcherait de légiférer à ce sujet, ou même de l'inclure dans ce projet de loi. J'imagine que vous n'aimez pas beaucoup que le gouvernement légifère sur ce que vous devez faire, mais il me semble que ce que chacun de vous faites représente une pratique exemplaire que l'on pourrait peut-être inclure dans la loi.

Qu'en pensez-vous?

Le président: Nous allons commencer par M. Beckerman.

M. Michael Beckerman: Comme je l'ai dit dans mon témoignage, la transparence est extrêmement importante, sur tous les rapports qu'un certain nombre de nos entreprises publient sur l'ensemble des demandes de données de la part des gouvernements. Nous avons peur que la loi puisse bloquer un certain nombre de ces rapports sur la transparence que nous trouvons très importants.

● (1300)

Le président: Madame Bickert.

Mme Monika Bickert: Nous respectons assurément toutes les lois applicables, mais nous sommes transparents parce que c'est important pour nous et pour ceux qui utilisent notre produit.

M. Sean Casey: Monsieur Beckerman, vous sembliez dire que la loi empêcherait les entreprises de télécommunications d'être plus transparentes. Vous ai-je bien compris?

M. Michael Beckerman: Selon ce que je comprends du projet de loi, une surveillance judiciaire pourrait bloquer la divulgation globale des demandes d'information.

M. Sean Casey: Merci.

Madame Zwibel, avez-vous bien dit que le projet de loi C-13 mènera à des appareils de localisation, y compris des logiciels, et qu'il pourrait permettre au gouvernement d'installer des logiciels malveillants pour localiser une personne? Avez-vous dit cela?

Mme Cara Zwibel: Oui, effectivement, c'était l'idée que j'avais des changements apportés aux définitions du dispositif de localisation et de l'enregistreur de données de transmission. J'ai les articles sous la main.

Ce sont des gens beaucoup plus doués en technologie que moi qui me l'ont récemment signalé. Un boursier postdoctoral à l'Université de Toronto, Christopher Parsons, a traité de ce changement dans son blogue.

Je crois savoir que changer les définitions... Avant, avec une autorisation judiciaire, on pouvait par exemple attacher un dispositif à une voiture pour pouvoir la suivre. Maintenant, la définition inclut des logiciels et des appareils que l'individu pourrait avoir sur lui, ce qui signifie qu'on peut installer des logiciels malveillants sur des appareils mobiles, un ordinateur ou même l'ordinateur interne d'une voiture.

À mon avis, c'est un changement important. Comme je l'ai dit, j'ai fait de mon mieux pour comprendre la technologie, mais ceux qui s'y connaissent mieux que moi ont laissé entendre que la police pourrait installer subrepticement des logiciels malveillants.

Le président: Monsieur Casey, il vous reste une minute.

M. Sean Casey: Madame Zwibel, vous savez sans doute que le projet de loi S-4, la Loi sur la protection des renseignements numériques, est actuellement à l'étude au Sénat. Je crois que le ministre a reconnu qu'il y avait un lien entre ce projet de loi et le projet de loi C-13, et pourtant à la fois le ministre et ses fonctionnaires ont soit hésité ou carrément refusé d'en discuter.

Pourquoi le lien entre ces deux projets de loi est-il important?

Mme Cara Zwibel: La disposition du projet de loi S-4 qui présente un lien avec le projet de loi C-13 est celle qui élargit les exceptions de la LPRPDE, dont j'ai parlé plus tôt.

À l'heure actuelle, la loi prévoit une exception. Dans certaines circonstances, une entreprise n'est pas tenue d'obtenir le consentement d'un individu avant de divulguer ses informations personnelles aux forces d'application de la loi ou à des organismes de l'État. Cette disposition en élargirait la portée pour inclure d'autres organismes qui pourraient demander de l'information en cas, par exemple, de violation de contrat présumée, de réclamations pour droit d'auteur et d'autres situations de cette nature.

Essentiellement, le problème c'est que des détenteurs d'information, des sociétés privées, deviennent arbitres dans un litige contractuel ou des questions qui concernent l'application de la loi. Dans ces domaines, la surveillance judiciaire est nécessaire.

La disposition du projet de loi C-13 qui a trait à l'immunité a évidemment un effet très important. À notre avis, si cette disposition du projet de loi S-4 est adoptée, les entreprises auront un incitatif de transmettre plus d'informations à la fois aux forces d'application de la loi et à d'autres qui en font la demande. Nous pensons qu'il faudrait faire le contraire.

Le président: Merci beaucoup pour vos questions et réponses.

J'aimerais remercier les témoins de leur présence aujourd'hui.

Pour la gouverne du comité, nous avons invité le commissaire à la protection de la vie privée. Il vient tout juste de confirmer qu'il sera des nôtres mardi pendant la première heure. Par la suite, nous passerons à l'examen article par article. Je sais que le Parti libéral a déjà présenté quelques amendements. Je vous prie de soumettre vos amendements avant demain midi, si c'est possible, pour que nous puissions nous préparer pour l'examen article par article mardi après-midi.

Il y aura encore une réunion sur ce sujet, puis nous allons enchaîner avec autre chose. Merci beaucoup pour votre patience et d'avoir été des nôtres aujourd'hui.

Sur ce, la séance est levée.