SENATE SÉNAT

CANADA

Second Session
Forty-first Parliament, 2013-14

Deuxième session de la
quarante et unième législature, 2013-2014

Proceedings of the Standing Senate Committee on

LEGAL AND CONSTITUTIONAL AFFAIRS

Chair:
The Honourable BOB RUNCIMAN

Wednesday, November 19, 2014
Thursday, November 20, 2014

Issue No. 21

Third and fourth meetings:

Bill C-13, An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act

WITNESSES:
(*See back cover*)

Délibérations du Comité sénatorial permanent des

AFFAIRES JURIDIQUES ET CONSTITUTIONNELLES

Président :
L'honorable BOB RUNCIMAN

Le mercredi 19 novembre 2014
Le jeudi 20 novembre 2014

Fascicule nº 21

Troisième et quatrième réunions :

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

TÉMOINS :
(*Voir à l'endos*)

51748-51760

STANDING SENATE COMMITTEE ON
LEGAL AND CONSTITUTIONAL AFFAIRS

The Honourable Bob Runciman, *Chair*

The Honourable George Baker, P.C., *Deputy Chair*

and

The Honourable Senators:

Batters	Frum
Boisvenu	Jaffer
* Carignan, P.C.	Joyal, P.C.
(or Martin)	McInnis
* Cowan	McIntyre
(or Fraser)	Plett
Dagenais	Rivest

*Ex officio members

(Quorum 4)

Change in membership of the committee:

Pursuant to rule 12-5, membership of the committee was amended as follows:

The Honourable Senator Plett replaced the Honourable Senator MacDonald (*November 6, 2014*).

COMITÉ SÉNATORIAL PERMANENT DES
AFFAIRES JURIDIQUES ET CONSTITUTIONNELLES

Président : L'honorable Bob Runciman

Vice-président : L'honorable George Baker, C.P.

et

Les honorables sénateurs :

Batters	Frum
Boisvenu	Jaffer
* Carignan, C.P.	Joyal, C.P.
(ou Martin)	McInnis
* Cowan	McIntyre
(ou Fraser)	Plett
Dagenais	Rivest

* Membres d'office

(Quorum 4)

Modification de la composition du comité :

Conformément à l'article 12-5 du Règlement, la liste des membres du comité est modifiée, ainsi qu'il suit :

L'honorable sénateur Plett a remplacé l'honorable sénateur MacDonald (*le 6 novembre 2014*).

Published by the Senate of Canada
Available on the Internet: http://www.parl.gc.ca

Publié par le Sénat du Canada
Disponible sur internet: http://www.parl.gc.ca

MINUTES OF PROCEEDINGS

OTTAWA, Wednesday, November 19, 2014
(49)

[*English*]

The Standing Senate Committee on Legal and Constitutional Affairs met at 4:17 p.m. this day, in room 257, East Block, the chair, the Honourable Bob Runciman, presiding.

Members of the committee present: The Honourable Senators Baker, P.C., Batters, Boisvenu, Dagenais, Frum, Jaffer, Joyal, P.C., McIntyre, Plett, and Runciman (10).

In attendance: Robin MacKay, analyst, Parliamentary Information and Research Service, Library of Parliament.

Also in attendance: The official reporters of the Senate.

Pursuant to the order of reference adopted by the Senate on Wednesday, November 5, 2014, the committee continued its study of Bill C-13, An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act. (*For complete text of the order of reference, see proceedings of the committee, Issue No. 20.*)

WITNESSES:

Criminal Lawyers' Association:

Leo Russomanno, Member and Criminal Defence Counsel;

Michael Spratt, Member and Criminal Defence Counsel.

Canadian Centre for Child Protection:

Lianna McDonald, Executive Director;

Monique St. Germain, General Counsel.

As individuals:

Andrea Slane, Associate Professor, University of Ontario Institute of Technology;

Michael Geist, Law Professor, University of Ottawa.

The chair made an opening statement.

Mr. Spratt, Mr. Russomano and Ms. McDonald each made a statement and, together with Ms. St. Germain, answered questions.

At 5:15 p.m., the committee suspended.

At 5:21 p.m., the committee resumed.

Ms. Slane and Mr. Geist each made a statement and answered questions.

At 6:15 p.m., the committee adjourned to the call of the chair.

ATTEST:

PROCÈS-VERBAUX

OTTAWA, le mercredi 19 novembre 2014
(49)

[*Traduction*]

Le Comité sénatorial permanent des affaires juridiques et constitutionnelles se réunit aujourd'hui, à 16 h 17, dans la salle 257 de l'édifice de l'Est, sous la présidence de l'honorable Bob Runciman (*président*).

Membres du comité présents : Les honorables sénateurs Baker, C.P., Batters, Boisvenu, Dagenais, Frum, Jaffer, Joyal, C.P., McIntyre, Plett et Runciman (10).

Également présent : Robin MacKay, analyste, Service d'information et de recherche parlementaires, Bibliothèque du Parlement.

Aussi présents : Les sténographes officiels du Sénat.

Conformément à l'ordre de renvoi adopté par le Sénat le mercredi 5 novembre 2014, le comité poursuit son 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. (*Le texte intégral de l'ordre de renvoi figure au fascicule n^{o} 20 des délibérations du comité.*)

TÉMOINS :

Criminal Lawyers' Association :

Leo Russomanno, membre et criminaliste;

Michael Spratt, membre et criminaliste.

Centre canadien de protection de l'enfance :

Lianna McDonald, directrice exécutive;

Monique St. Germain, avocate-conseil.

À titre personnel :

Andrea Slane, professeure agrégée, Institut universitaire de technologie de l'Ontario;

Michael Geist, professeur de droit, Université d'Ottawa.

Le président prend la parole.

MM. Spratt et Russomano ainsi que Mme McDonald font chacun une déclaration puis, avec Mme St. Germain, répondent aux questions.

À 17 h 15, la séance est suspendue.

À 17 h 21, la séance reprend.

Mme Slane et M. Geist font chacun une déclaration, puis répondent aux questions.

À 18 h 15, le comité s'ajourne jusqu'à nouvelle convocation de la présidence.

ATTESTÉ :

OTTAWA, Thursday, November 20, 2014
(50)

[*English*]

The Standing Senate Committee on Legal and Constitutional Affairs met at 10:30 a.m. this day, in room 257, East Block, the chair, the Honourable Bob Runciman, presiding.

Members of the committee present: The Honourable Senators Baker, P.C., Batters, Boisvenu, Dagenais, Frum, Joyal, P.C., McInnis, McIntyre, Plett and Runciman (10).

In attendance: Robin MacKay, analyst, Parliamentary Information and Research Service, Library of Parliament.

Also in attendance: The official reporters of the Senate.

Pursuant to the order of reference adopted by the Senate on Wednesday, November 5, 2014, the committee continued its study of Bill C-13, An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act. (*For complete text of the order of reference, see proceedings of the committee, Issue No. 20.*)

WITNESSES:

Canadian Bar Association:

Tony Paisana, Executive Member, Criminal Justice Section (by video conference).

Office of the Privacy Commissioner of Canada:

Daniel Therrien, Privacy Commissioner of Canada;

Patricia Kosseim, Senior General Counsel and Director General;

Daniel Caron, Legal Counsel.

Boys and Girls Clubs of Canada:

Rachel Gouin, Director, Research and Public Policy;

Fahd Alhattab, Alumnus.

Bully Free Community Alliance:

Basiliki Schinas-Vlasis, Co-Founder;

Gwyneth Anderson, Co-Founder.

The chair made an opening statement.

Mr. Paisana made a statement and answered questions.

At 11:09 a.m., the committee suspended.

At 11:15 a.m., the committee resumed.

Mr. Therrien made a statement and, together with Ms. Kosseim, answered questions.

At 11:49 a.m., the committee suspended.

At 12:08 p.m., the committee resumed.

OTTAWA, le jeudi 20 novembre 2014
(50)

[*Traduction*]

Le Comité sénatorial permanent des affaires juridiques et constitutionnelles se réunit aujourd'hui, à 10 h 30, dans la pièce 257 de l'édifice de l'Est, sous la présidence de l'honorable Bob Runciman (*président*).

Membres du comité présents : Les honorables sénateurs Baker, C.P., Batters, Boisvenu, Dagenais, Frum, Joyal, C.P., McInnis, McIntyre, Plett et Runciman (10).

Également présent : Robin MacKay, analyste, Service d'information et de recherche parlementaires, Bibliothèque du Parlement.

Aussi présents : Les sténographes officiels du Sénat.

Conformément à l'ordre de renvoi adopté par le Sénat le mercredi 5 novembre 2014, le comité poursuit son 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 (*Le texte intégral de l'ordre de renvoi figure au fascicule nº 20 des délibérations du comité.*)

TÉMOINS :

Association du Barreau canadien :

Tony Paisana, membre de l'exécutif, Section du droit pénal (par vidéoconférence).

Commissariat à la protection de la vie privée du Canada :

Daniel Therrien, commissaire à la protection de la vie privée du Canada;

Patricia Kosseim, avocate générale principale et directrice générale;

Daniel Caron, conseiller juridique.

Clubs garçons et filles du Canada :

Rachel Gouin, directrice, Recherche et politiques publiques;

Fahd Alhattab, ancien membre.

Bully Free Community Alliance :

Basiliki Schinas-Vlasis, cofondatrice;

Gwyneth Anderson, cofondatrice.

Le président prend la parole.

M. Paisana fait une déclaration, puis répond aux questions.

À 11 h 9, la séance est suspendue.

À 11 h 15, la séance reprend.

M. Therrien fait une déclaration puis, avec Mme Kosseim, répond aux questions.

À 11 h 49, la séance est suspendue.

À 12 h 8, la séance reprend.

Mr. Alhattab, Ms. Schinas-Vlasis and Ms. Anderson each made a statement and, together with Ms. Gouin, answered questions.

At 1:05 p.m., the committee adjourned to the call of the chair.

ATTEST:

M. Alhattab ainsi que Mmes Schinas-Vlasis et Anderson font chacun une déclaration puis, avec Mme Gouin, répondent aux questions.

À 13 h 5, le comité s'ajourne jusqu'à nouvelle convocation de la présidence.

ATTESTÉ :

La greffière du comité,

Shaila Anwar

Clerk of the Committee

EVIDENCE

OTTAWA, Wednesday, November 19, 2014

The Standing Senate Committee on Legal and Constitutional Affairs, to which was referred Bill C-13, An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act, met this day at 4:17 p.m. to give consideration to the bill.

Senator Bob Runciman (*Chair*) in the chair.

[*English*]

The Chair: Good day. Welcome colleagues, invited guests and members of the general public who are following today's proceedings of the Standing Senate Committee on Legal and Constitutional Affairs. We are meeting today to continue our study of Bill C-13, An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act.

As a reminder to those watching, these committee hearings are open to the public and are also available via webcast on the parl.gc.ca website. You can find more information on the schedule of witnesses on that same website, under "Senate Committees."

To begin today's proceedings, please welcome, for our first panel, from the Criminal Lawyers' Association, Leo Russomanno, who is a member of the association and criminal defence counsel; and Michael Spratt, member of the association as well and a criminal defence counsel.

From the Canadian Centre for Child Protection, we welcome Lianna McDonald, the Executive Director; and Monique St. Germain, General Counsel.

I understand we have agreed to a format for opening statements. Michael Spratt, the floor is yours.

Michael Spratt, Member and Criminal Defence Counsel, Criminal Lawyers' Association: As you may know, the Criminal Lawyers' Association is a non-profit organization comprised of over a thousand criminal defence counsel from across Canada. The CLA supports legislation that's fair, modest, constitutional and supported by the evidence.

Since I'm splitting my time with Mr. Russomanno, I'll cut right to the chase. The CLA simply can't support Bill C-13 in its current form. Bill C-13, in our view, is a Trojan Horse for the reckless expansion of the state's ability to collect and catalogue information. Bill C-13, along with Bill S-4, represents a dangerous and, in our opinion, unconstitutional pattern of erosion of privacy.

Bill C-13 disregards clear directions and judgments from the Supreme Court of Canada, and the lawful access provisions are likely unconstitutional.

TÉMOIGNAGES

OTTAWA, le mercredi 19 novembre 2014

Le Comité sénatorial permanent des affaires juridiques et constitutionnelles, auquel a été renvoyé le 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, se réunit aujourd'hui à 16 h 17 pour examiner le projet de loi.

Le sénateur Bob Runciman (*président*) occupe le fauteuil.

[*Traduction*]

Le président : Bonjour. Bienvenue à mes collègues et aux membres du public qui suivent cette audience du Comité sénatorial permanent des affaires juridiques et constitutionnelles. Nous nous réunissons aujourd'hui pour poursuivre 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.

Je rappelle à ceux qui regardent, que les audiences du comité sont ouvertes au public et qu'on peut les visionner sur le site web parl.gc.ca. Vous pouvez trouver de l'information supplémentaire sur le calendrier des exposés des témoins sur le même site web, sous la rubrique « Comités du Sénat ».

Pour commencer aujourd'hui, je vous prie d'accueillir notre premier groupe de témoins. Nous entendrons deux criminalistes membres de la Criminal Lawyers' Association, Leo Russomanno et Michael Spratt.

Nous souhaitons aussi la bienvenue aux représentantes du Centre canadien de protection de l'enfance : Lianna McDonald, directrice exécutive, et Monique St. Germain, avocate-conseil.

Si j'ai bien compris, nous nous sommes entendus sur l'ordre des exposés. Michael Spratt, vous avez la parole.

Michael Spratt, membre et criminaliste, Criminal Lawyers' Association : Comme vous le savez peut-être, la Criminal Lawyers' Association est un organisme sans but lucratif comptant plus d'un millier d'avocats de la défense à l'échelle du Canada. La CLA appuie les mesures législatives justes, modestes, constitutionnelles et s'appuyant sur des preuves.

Étant donné que je partage mon temps avec M. Russomanno, je vais aller droit au but. La CLA ne peut tout simplement pas appuyer le projet de loi C-13 dans sa forme actuelle. D'après nous, le projet de loi C-13 est un cheval de Troie qui favorisera l'explosion irresponsable de la capacité de l'État de recueillir et de cataloguer de l'information. Le projet de loi C-13, avec le projet de loi S-4, représente une façon dangereuse et, d'après nous, inconstitutionnelle d'éroder le droit à la vie privée.

Le projet de loi C-13 bafoue les orientations claires et les décisions de la Cour suprême, et les dispositions visant l'accès légal à l'information sont vraisemblablement inconstitutionnelles.

I will speak about the unprincipled and low standards for the production orders regarding transmission data, and Mr. Russomanno will speak about the issue of immunity for voluntary disclosure.

In the time since this matter was before the House of Commons committee, the Supreme Court of Canada released its decision in *Spencer*. *Spencer* makes crystal clear what should have already been apparent. Metadata, transmission data, is personal and sensitive information. The Supreme Court found that there's a reasonable expectation of privacy with this sort of information. That was already the case. The Supreme Court made that clear in *Vu*, when describing metadata as revealing intimate details about a user's interests, habits and identity. Interestingly enough, in the *Vu* case, federal prosecutors argued that no warrant was actually required to search a computer. They were wrong in that case, and Bill C-13 is wrong in its current form.

Spencer confirmed, as I said, what was clear in *Vu*. The court held that there is a privacy interest in metadata. This type of data can reveal core biographical information, and metadata, therefore, engages a high level of informational privacy. That's plain wording of *Spencer*.

It should be noted that *Spencer* was only about connecting an IP address to an individual. Bill C-13 allows much more than that. Who you are, where you are, where you've been, what you've searched for, who you spoke to, all of this type of information can be provided under the production order in Bill C-13.

The minister testified before this committee and told you that the reasonable suspicion threshold reflects a low level of intrusiveness of power in relation to both the quality and the quantity of information. He said that lower expectations of privacy are triggered by such information. Quite simply, he was wrong. The Supreme Court of Canada debunked that characterization and one of the other common refrains and talking points, that metadata is only analogous to phone book information. The Supreme Court of Canada has also made it clear that reasonable suspicion should only be reserved for cases with reduced expectations of privacy.

The Supreme Court's comments about the heightened privacy interest inherent in Internet data and metadata are simply incompatible with the lower standard of reasonable suspicion contained in Bill C-13. This is especially so given that there are very little controls in Bill C-13 about the retention and the use that that data can be put to. One need look no further than the John Howard Society report and the Canadian Civil Liberties Association report on police record checks to see the devastating impact that can manifest when there is little or no control over the use and access of information by the police.

Je vais parler des normes faibles et dénuées de principe concernant les ordonnances de communication visant les données de transmission, et M. Russomanno parlera de la question de l'immunité en cas de divulgation volontaire.

Le comité de la Chambre des communes avait été saisi de cette question quand la Cour suprême du Canada a rendu sa décision dans l'affaire *Spencer*. Cet arrêt rend on ne peut plus claire une chose qui aurait déjà dû être évidente. Les métadonnées, les données de transmissions, constituent de l'information personnelle et délicate. La Cour suprême a conclu qu'on peut raisonnablement s'attendre à ce que ce type d'information soit protégé. Il en était déjà ainsi. La Cour suprême l'a souligné sans équivoque dans l'arrêt *Vu*, quand elle a décrit les métadonnées comme étant des détails intimes sur les intérêts, les habitudes et l'identité d'un utilisateur. Fait intéressant, dans l'arrêt *Vu*, les procureurs fédéraux ont fait valoir qu'il ne fallait pas de mandat pour fouiller un ordinateur. Ils étaient dans l'erreur, et le projet de loi C-13 est erroné dans sa forme actuelle.

L'arrêt *Spencer* a confirmé, comme je l'ai dit, ce qui était évident dans l'arrêt *Vu*. La cour a confirmé que les métadonnées soulèvent des préoccupations relatives à la vie privée. De telles données peuvent révéler de l'information biographique fondamentale, et les métadonnées font intervenir, dans une grande mesure, l'aspect informationnel du droit à la vie privée. C'est exactement ainsi que c'est exprimé dans l'arrêt *Spencer*.

Il faut souligner que l'arrêt *Spencer* ne porte que sur le lien entre une adresse IP et une personne. Le projet de loi C-13 permet beaucoup plus que cela. La personne que vous êtes, le lieu où vous êtes, là où vous êtes allé, ce que vous avez cherché, les personnes auxquelles vous avez parlé — toute cette information peut être fournie en application des dispositions du projet de loi C-13 visant l'ordonnance de communication.

Le ministre a témoigné devant le comité et vous a dit que les critères cadrent avec le faible degré d'atteinte à la vie privée associé à ces pouvoirs, tant en ce qui a trait à la qualité et à la quantité de l'information obtenue qu'aux attentes concernant la protection de ces renseignements. Il a tout simplement tort. La Cour suprême a démenti cette interprétation, ainsi qu'un des autres refrains qu'on entend souvent, celui selon lequel les métadonnées se comparent tout simplement à l'information qu'on trouve dans un répertoire téléphonique. La Cour suprême du Canada a aussi précisé clairement qu'il ne faut réserver le doute raisonnable qu'aux cas où les attentes relatives à la protection de la vie privée sont réduites.

Les observations de la Cour suprême concernant le caractère privé des données sur Internet et des métadonnées sont tout simplement incompatibles avec les faibles normes de doute raisonnable que comporte le projet de loi C-13. C'est particulièrement le cas, étant donné que le projet de loi C-13 comporte très peu de modes de contrôle permettant de comparer la conservation et l'utilisation des données. Il n'est pas nécessaire de chercher plus loin que le rapport de la Société John Howard et le rapport de l'Association canadienne des libertés civiles concernant les vérifications de dossiers de la police pour

Bill C-13 purports to be concerned with tackling cyberbullying and stopping the spread of intimate images online. The real tragedy is that those provisions are indeed necessary and laudable and should be proceeded with. However, in reality, that aspect takes up only a small amount of Bill C-13.

On balance, Bill C-13 sacrifices privacy in favour of expanded police powers and liberal disclosure standards.

Leo Russomanno, Member and Criminal Defence Counsel, Criminal Lawyers' Association: Thanks for having me here. I just want to provide some general impressions from reading over the bill.

Surely I'm not the only one who detects the extreme irony of a bill that purports to protect the online privacy of Canadians from would-be predators but, at the same time, at the back end of the bill basically opens the door to a wide-scale government intrusion on people's privacy. Surely I'm not the genius here who figured this out and detected the irony here in this bill.

We have a problem, in my submission, with the dialogue that goes on when we talk about the Canadian Charter of Rights and Freedoms. The only cases we ever hear about involve evidence being seized that leads to a criminal case. The obvious reality, and something the Supreme Court has painstakingly recognized, is that the Charter is a document that protects all of us. Those of us who don't end up before the criminal courts deserve to have our rights protected as well, and those people who do end up in criminal courts serve as proxies for all of us who have to have our rights protected.

So this bill proposes to provide incentives to service providers to voluntarily hand over Internet service data. We're met with a unique opportunity here, where the Supreme Court has, in the wake of this bill being introduced, actually decided a case that is more or less on all fours with the subject matter of this legislation. The Supreme Court has spoken clearly, and when I hear Minister MacKay discuss the impact of this decision, I don't know how many ways I can say that he is just completely wrong in his interpretation of how this case applies to the subject matter. It is absolutely wrong. Voluntary disclosure will prove to be contrary to the Charter, given what the Supreme Court has already said in *Spencer*. They have already said that there is a reasonable expectation of privacy with such information. That means that, by definition, section 8 applies, and a warrantless search would be unreasonable.

So we need to actually move forward, interpret this case properly, interpret the *Spencer* case, interpret the *Vu* case and not waste our time with a future Charter challenge that has a high chance of success. I ask that this committee keep in mind the true value of the Charter when considering this legislation.

constater l'effet dévastateur de l'insuffisance ou de l'absence de contrôle sur l'utilisation de l'information et l'accès à l'information de la police.

On prétend que le projet de loi C-13 cherche à s'attaquer à la cyberintimidation et à la distribution d'images intimes en ligne. La vraie tragédie, c'est que ces dispositions sont en fait nécessaires et louables, et qu'il faudrait les adopter. Cependant, en réalité, cet aspect ne représente qu'une petite partie du projet de loi C-13.

Dans l'ensemble, le projet de loi C-13 sacrifie la protection de la vie privée au profit de l'augmentation des pouvoirs de la police et de l'adoption de normes de divulgation libérales.

Leo Russomanno, membre et criminaliste, Criminal Lawyers' Association : Je vous remercie de m'avoir invité. Je veux simplement donner mes impressions générales à la suite de la lecture du projet de loi.

Je ne suis certainement pas le seul à percevoir l'ironie d'un projet de loi qui prétend protéger la vie privée en ligne des Canadiens des prédateurs, tout en ouvrant la porte à une intrusion gouvernementale à grande échelle dans la vie privée des gens. Je ne suis certainement pas le génie qui a compris cela et qui a vu l'ironie derrière ce projet de loi.

À mon avis, nous avons un problème avec le dialogue sur la Charte canadienne des droits et libertés. Les seuls cas dont nous entendons parler visent des preuves saisies qui mènent à une affaire criminelle. La réalité évidente, que la Cour suprême a péniblement reconnue, c'est que la Charte est là pour nous protéger tous. Ceux d'entre nous qui n'aboutissent pas devant les cours criminelles méritent aussi que leurs droits soient protégés. Et les personnes qui finissent devant les cours criminelles nous représentent tous, nous, dont les droits sont protégés.

Ce projet de loi propose donc des moyens d'encourager les fournisseurs de services à donner volontairement des données sur les services Internet. Nous avons ici une occasion unique, alors qu'à la suite du dépôt de ce projet de loi, la Cour suprême a rendu une décision qui porte plus ou moins sur ce que ce projet de loi couvre. La Cour suprême a parlé clairement, et quand j'entends le ministre MacKay discuter des incidences de cette décision, je ne sais pas comment dire qu'il a tout à fait tort dans son interprétation de la façon dont cet arrêt s'applique au sujet à l'étude. C'est complètement erroné. La divulgation volontaire va se révéler contraire à la Charte, compte tenu de ce que la Cour suprême a déjà dit dans l'arrêt *Spencer*. Elle a déjà dit qu'il y a une attente raisonnable de respect de la vie privée à l'égard de cette information. Cela signifie, par définition, que l'article 8 s'applique et qu'une fouille sans mandat ne serait pas raisonnable.

Il nous faut donc aller de l'avant et interpréter cet arrêt convenablement, interpréter l'arrêt *Spencer*, et l'arrêt *Vu*, et ne pas perdre de temps avec de futures contestations axées sur la Charte qui risquent fort de l'emporter. Je demande au comité de garder à l'esprit la réelle valeur de la Charte au moment de se pencher sur ce projet de loi.

The Chair: Thank you, sir.

Ms. McDonald.

Lianna McDonald, Executive Director, Canadian Centre for Child Protection: Mr. Chair and distinguished members of this committee, I thank all very much for giving us this opportunity to provide a presentation on Bill C-13.

My name is Lianna McDonald, and I am the Executive Director of the Canadian Centre for Child Protection, a registered charity providing national programs and services related to the personal safety of all children. Joining me today is my colleague and our general counsel, Monique St. Germain, and she will be here to answer any questions that you also may have.

Our goal today is to provide support for Bill C-13. We will offer testimony based on our role in operating Cybertip.ca, which is Canada's national tip line to report the online sexual exploitation and abuse of children. It has been through this work that we see the most brutal behaviours towards children. We have also seen teens trying to navigate the social media fallout from a sexual picture or trying to cope with the aftermath of a sexual crime that has been recorded. What we have witnessed firsthand, and all too often, is the collision between sexual exploitation, technology and bullying.

Through Cybertip, we have received over 125,000 reports regarding the sexual abuse and exploitation of children, the majority of which deal with child pornography complaints. Of those reports to the tip line, approximately 4 per cent are submitted by young people who are coming in as both the victim and the reporting person. Many of these reports contain sexual images and videos being created and distributed electronically among their peers, sometimes as a form of bullying. In some cases, the images were voluntarily shared and in others the images were coerced or taken without the child's knowledge.

The number one request from those impacted by a sexual image being shared online is to get the content removed. These youth are desperate to get humiliating photos or videos of themselves off of the Internet and have had nowhere to turn to get the help that they need. Over the last year and a half, we have seen and received at least a dozen reports from youth threatening either self-harm or suicide in relation to the distribution of a sexual image. We believe Bill C-13 will help address the dilemma for content networks when being asked to remove the content from their service. Such action can reduce the victimization of a young person significantly.

To respond to these complex cases, in 2012 we released a guide addressing self-peer exploitation commonly known as "sexting," which is a resource intended to assist schools and families who are dealing with the negative impact of a photo or video of a young person that has ended up online. This resource was in the final

Le président : Merci, monsieur.

Madame McDonald.

Lianna McDonald, directrice exécutive, Centre canadien de protection de l'enfance : Monsieur le président, distingués membres du comité, je vous remercie beaucoup de me donner l'occasion de faire un exposé sur le projet de loi C-13.

Je suis Lianna McDonald, et je suis la directrice exécutive du Centre canadien de protection de l'enfance, un organisme de bienfaisance enregistré qui propose des programmes et des services nationaux visant la sécurité personnelle de tous les enfants. Je suis accompagnée de ma collègue, notre avocate-conseil, Monique St. Germain, qui pourra répondre à toutes vos questions.

Notre but, aujourd'hui, est d'exprimer notre appui au projet de loi C-13. Nous témoignerons en nous fondant sur le rôle que nous jouons dans le fonctionnement de Cyberaide.ca, la centrale canadienne de signalement des cas d'exploitation sexuelle d'enfants sur Internet. C'est en exécutant ce travail que nous constatons les comportements les plus brutaux envers les enfants. Nous avons aussi vu des adolescents chercher à se tirer du désastre causé par une photo de nature sexuelle circulant sur les réseaux sociaux ou à atténuer les conséquences d'un crime sexuel qui a été enregistré. Ce que nous constatons directement, et trop souvent, c'est la collision entre l'exploitation sexuelle, la technologie et l'intimidation.

Grâce à Cyberaide.ca, nous avons reçu plus de 125 000 signalements de violence et d'exploitation sexuelle d'enfants dont la majorité est composée de plaintes de pornographie juvénile. Environ 4 p. 100 de ces signalements sont faits par des jeunes qui sont eux-mêmes les victimes des événements signalés. Bon nombre de ces signalements portent sur des images et des vidéos de nature sexuelle qui ont été créées et distribuées électroniquement entre pairs, parfois pour faire de l'intimidation. Dans certains cas, les images ont été partagées volontairement, alors que dans d'autres, elles ont été obtenues sous la contrainte ou à l'insu de l'enfant.

Ce que les personnes touchées par une image de nature sexuelle partagée en ligne demandent principalement, c'est le retrait de ce contenu. Ces jeunes veulent désespérément que les photos ou vidéos humiliantes d'eux soient retirées d'Internet et n'ont personne vers qui se tourner pour obtenir l'aide qu'il leur faut. Au cours de la dernière année et demie, nous avons reçu des dizaines de signalements de jeunes qui menacent de se faire du mal ou de s'enlever la vie à cause du partage d'une image de nature sexuelle. Nous croyons que le projet de loi C-13 va résoudre le dilemme des réseaux de contenu, quand on leur demande de retirer le contenu de leur service. De telles mesures peuvent nettement réduire la victimisation d'une jeune personne.

Pour réagir à ces cas complexes, nous avons publié, en 2012, un guide portant sur l'autoexploitation juvénile, ou ce que l'on appelle couramment les « sextos ». C'est une ressource dont le but est d'aider les écoles et les familles aux prises avec les conséquences négatives de la photo ou de la vidéo d'une jeune

editing stage when Amanda Todd took her life, and since publication, we have received over 10,000 requests for copies of this guide.

Also, in early 2013 we launched a resource called NeedHelpNow.ca, a website aimed at youth to provide specific information about this issue and where to get help. On average, we receive 16,000 unique page views a month, with the most popular page being "Steps you can take to remove content from the Internet." To further our education and these educational resources, we have recently created new guides for Grade 7 to 10 students that deal with the issues of personal boundaries, sexual consent and how to respond to these harmful situations.

While these and other resources are important, we know this is not enough. Prevention is not the same as intervention. When it comes to this issue, we do need both.

To this end, we support Bill C-13 for the following reasons: First, we believe an intimate image offence is much more appropriate than a child pornography offence in circumstances involving youth; second, we support that the offence covers victims of all ages; and, third, we welcome provisions that facilitate the removal and deletion of images.

Technology has become a powerful weapon and the ammunition of choice for those who wish to hide behind the protected cloak of anonymity. New technologies make it much easier to harass and participate in a toxic digital frontier where ongoing biases about sexual misconduct collide with unrealistic expectations of adolescent behaviour, fuelled by the misuse of technology.

While we are sophisticated enough not to place the blame solely on technology, we should be rightly committed to understanding its role in the commission of offences and how as we as a nation choose to respond and modernize laws to adequately address new types of criminal behaviour.

In closing, we know that the issues youth are facing today are far beyond what we might have imagined. We know that too many young people are suffering silently and we have lost too many kids to suicide, those who felt that there was no way out, no help, and that no one could make a difference. This is absolutely not okay. Our children deserve better.

Thank you.

The Chair: Thank you all for your opening statements. We have a long list of questioners, beginning with the committee's deputy chair, Senator Baker.

personne qui a abouti en ligne. Cette ressource en était à la dernière étape d'édition quand Amanda Todd s'est enlevé la vie. Depuis sa publication, nous avons reçu plus de 10 000 demandes d'exemplaires de ce guide.

Au début de 2013, nous avons aussi lancé une ressource appelée AidezMoiSVP.ca, un site web qui fournit de l'information précise aux jeunes sur ce problème et sur l'endroit où obtenir de l'aide. En moyenne, nous avons 16 000 visiteurs uniques par mois, et la page la plus populaire est celle des « Mesures à prendre pour retirer des images d'Internet ». Pour pousser plus loin l'éducation et les ressources servant à cette fin, nous avons récemment créé de nouveaux guides pour les élèves de la 7e à la 10e année. Ils traitent des questions de limites personnelles et de consentement sexuel, et donnent des façons de réagir à des situations qui présentent des risques.

Ces guides et les autres ressources qui existent sont importants, mais nous savons que cela ne suffit pas. La prévention, ce n'est pas comme l'intervention. Avec ce problème, il faut les deux.

À cette fin, nous appuyons le projet de loi C-13 pour les raisons suivantes : premièrement, nous croyons qu'une infraction liée à une image intime est beaucoup plus appropriée qu'une infraction liée à la pornographie juvénile, dans les cas où des jeunes sont impliqués; deuxièmement, nous sommes d'accord pour dire que l'infraction doit couvrir les victimes de tous les âges; et troisièmement, nous nous réjouissons des dispositions qui facilitent le retrait et la suppression des images.

La technologie est devenue une arme puissante, et elle donne des munitions de choix à ceux qui veulent se protéger derrière l'anonymat. Les nouvelles technologies facilitent énormément le harcèlement et la participation à une frontière numérique toxique où se heurtent, d'un côté, les préjugés durables sur l'inconduite sexuelle et de l'autre, les attentes irréalistes concernant le comportement des adolescents, le tout alimenté par la mauvaise utilisation de la technologie.

Nous pouvons comprendre qu'il ne faut pas jeter le blâme uniquement sur la technologie, mais nous devons vraiment être déterminés à comprendre le rôle qu'elle joue dans la perpétration d'infractions et dans la façon dont une nation choisit de réagir et de moderniser les lois de manière à traiter convenablement ces nouveaux types de comportements criminels.

En conclusion, nous savons que les problèmes que les jeunes rencontrent aujourd'hui dépassent de loin ce que nous aurions pu imaginer. Nous savons que trop de jeunes souffrent en silence, et le suicide nous a enlevé trop de jeunes, des jeunes qui ne voyaient pas d'issue, pas d'aide, personne qui pouvait changer les choses. C'est complètement inacceptable. Nos enfants méritent mieux que cela.

Merci.

Le président : Merci à vous tous de vos exposés. Nous avons une longue liste de personnes qui ont des questions, à commencer par le vice-président, le sénateur Baker.

Senator Baker: Thank you to the presenters for their excellent presentations. They were thoroughly enjoyed and appreciated.

My question is directed toward Mr. Russomanno or Mr. Spratt. First, I would like to congratulate them on the great contribution they make as litigators. Almost on a daily basis one can read the case law that they participate in.

I have two questions. My first question is this: How do you answer a person who says we have PIPEDA, the act that we passed in 2000, 2001. I recall the day we did it. Subsection 7(3) of that act states that "an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is . . . requested for the purpose of enforcing any law of Canada . . . carrying out an investigation relating to the enforcement of any such law . . . ." It is an open-ended exception to the provisions, I would say, of PIPEDA.

When you look at 487.012 that we are displacing here today, in regard to a production order, one sees words to the effect that a judge has "reasonable grounds to believe that" a police officer has a suspicion. Now without getting into how the courts have interpreted that phrase, how do you answer people who say that we are not really going down the road that you're suggesting, because already in PIPEDA and in the Criminal Code provision we have, the word "suspicion" is there very clearly. How do you answer that?

Mr. Spratt: Looking at what's already in the Criminal Code can give some context for what should be done in this case. For example, getting a production order for a telephone company to list the numbers that you've dialed, a number recorder warrant, requires reasonable suspicion. That has been an acceptable standard, because the information you get are the numbers dialed.

When you look at the information that can be disseminated and disclosed in this bill, it's more than that. I'm sure the committee will hear from some experts, perhaps even today, who can talk about metadata, and the courts have made pronouncements on that.

When you're looking at that in context with PIPEDA, we may have to do what the Supreme Court did in *Spencer*. The whole purpose of PIPEDA is to increase the protection of personal information. In the context of voluntary disclosure, the Supreme Court was quite clear that you can't use a declaratory provision in the Criminal Code combined with a statute that's supposed to enhance and increase protection of personal information to do the opposite.

Le sénateur Baker : Merci à nos témoins pour leurs excellents exposés. Nous les avons beaucoup appréciés.

Je pose ma question à M. Russomanno ou à M. Spratt. Premièrement, je veux les féliciter de leur formidable contribution à titre de plaideurs. Presque tous les jours, on peut lire des décisions rendues dans des causes auxquelles ils participent.

J'ai deux questions. Premièrement, comment répondez-vous à une personne qui dit que nous avons la Loi sur la protection des renseignements personnels et les documents électroniques, que nous avons adoptée en 2000 ou 2001? Je me rappelle le jour où nous l'avons fait. Le paragraphe 7(3) de la loi dit que « l'organisation ne peut communiquer de renseignement personnel à l'insu de l'intéressé et sans son consentement » que si « la communication est demandée aux fins du contrôle d'application du droit canadien... de la tenue d'enquêtes liées à ce contrôle d'application... » C'est une exception ouverte aux dispositions de la Loi sur la protection des renseignements personnels et les documents électroniques, je dirais.

À l'article 487.012 concernant une ordonnance de communication, le libellé est tel qu'un juge devrait avoir « des motifs raisonnables de soupçonner » qu'un agent de police a des soupçons. Je ne veux pas que nous parlions de la façon dont les tribunaux interprètent cette phrase, mais j'aimerais que vous me disiez ce qu'il faut répondre à quelqu'un qui dit que nous ne prenons pas vraiment la direction que vous dites, parce que le principe du soupçon est déjà très clair dans la Loi sur la protection des renseignements personnels et les documents électroniques et dans le Code criminel. Comment répondez-vous à cela?

M. Spratt : Vous obtiendrez dans le Code criminel un certain contexte pour ce qu'il faut faire dans ce cas. Par exemple, pour obtenir une ordonnance de communication obligeant une compagnie de téléphone à produire une liste des numéros que vous avez composés — un mandat pour les enregistreurs de numéros de téléphone —, il faut des motifs raisonnables de soupçonner quelque chose. C'est une norme acceptée, parce que l'information que vous obtenez, ce sont les numéros de téléphone composés.

L'information qui peut être diffusée et divulguée dans ce projet de loi dépasse cela. Je suis sûr que le comité entendra des experts, peut-être aujourd'hui, parler de métadonnées, et les tribunaux ont tranché à ce sujet.

Dans le contexte de la Loi sur la protection des renseignements personnels et les documents électroniques, il sera peut-être nécessaire de faire comme la Cour suprême dans l'arrêt *Spencer*. Le but de la Loi sur la protection des renseignements personnels et les documents électroniques est de resserrer la protection des renseignements personnels. Dans le contexte de la divulgation volontaire, la Cour suprême a très clairement dit qu'on ne peut combiner une disposition déclaratoire du Code criminel à une loi dont le but est de resserrer et d'améliorer la protection de l'information personnelle dans le but de faire le contraire.

Senator Baker: You have used the term "reasonable suspicion," and I know why you have used that term. I've been on committees for 40 years here on Parliament Hill, and it's a term that has crept into our law mainly in the provisions relating to Controlled Drugs and Substances Act searches. A dog sniff is a search. You need a reasonable suspicion for that search.

That has been adjudicated recently in 2013 by the Supreme Court of Canada. You're nodding your head. You probably know the case. You have the case there that I'm referring to. You're very well up on our case law, Mr. Spratt.

Is this really a new era? To justify the dog sniff search, which, under the Supreme Court decision in *Kang-Brown*, is judged to be a search, a reasonable suspicion is the standard to be used, which as you will point out is less than "reasonable grounds to believe" but more than just a suspicion. Are we really going down a new road here with the provisions in this bill?

Mr. Spratt: We are going on down a new road.

Senator Baker: What is the case, by the way, I was referring to?

Mr. Spratt: There is *Kang-Brown*, and the case I brought is one that follows it.

Senator Baker: Last year.

Mr. Spratt: *R. v. Chehil*, from 2013, another dog sniffing case, and they talk about reasonable suspicion.

You're quite right. The courts have said that when there is a low expectation of privacy in the information, for example, the smell that comes out of your luggage at an airport or in a school, under those circumstances reasonable suspicion might suffice, or grounds to request a breathalyzer, roadside breath testing, or, as we talked about, to obtain telephone numbers.

The reasonable suspicion standard has been judicially approved in those cases because the privacy interest is low. If you go back to *Hunter v. Southam*, the court said that when you're balancing these interests, the right to privacy against the right of a state to investigate offences, searches based on reasonable suspicion can only be justified where there is a low privacy interest, a reduced privacy interest, which of course is in dramatic contrast to what the Supreme Court has said in both *Vu* and *Spencer* with respect to metadata.

It doesn't take a genius to put two and two together in that case that we're dealing with information that has a high privacy value, and we're dealing with a standard that is only appropriate when there is a low privacy value.

The Chair: I have to stop you there, and we have to move to Senator Plett.

Senator Plett: Thank you to our witnesses.

Le sénateur Baker : Vous avez employé l'expression « soupçon raisonnable ». Je sais pourquoi. J'ai fait partie de comités pendant 40 ans, ici, sur la Colline. Cette expression s'est glissée dans notre droit, principalement dans les dispositions concernant les perquisitions et les fouilles sous le régime de la Loi réglementant certaines drogues et autres substances. L'emploi d'un chien renifleur constitue une perquisition. Pour la faire, il faut un soupçon raisonnable.

En 2013, la Cour suprême a tranché. Vous hochez la tête. Vous connaissez probablement l'affaire. Vous avez le jugement sous les yeux. Vous êtes très au courant de notre jurisprudence, monsieur Spratt.

Les temps sont-ils vraiment nouveaux? Pour justifier la perquisition par un chien renifleur, qui, d'après l'arrêt *Kang-Brown* de la Cour suprême constitue une perquisition, le soupçon raisonnable est le critère à employer, moins exigeant, direz-vous, que le motif raisonnable de croire, mais plus que le simple soupçon. Est-ce que les dispositions de ce projet de loi nous entraînent en terrain inconnu?

M. Spratt : C'est ce qu'elles font.

Le sénateur Baker : À propos, quel était cet arrêt dont je parlais?

M. Spratt : L'arrêt *Kang-Brown*, et j'ai ici celui qui a suivi.

Le sénateur Baker : L'année dernière.

M. Spratt : *R. c. Chehil*, en 2013, une autre affaire de chien renifleur. Et il y est question de soupçon raisonnable.

Vous avez tout à fait raison. Les tribunaux ont dit que pour de faibles attentes relativement au caractère privé de l'information, par exemple de l'odeur qui se dégage des bagages dans une aérogare ou une école, un soupçon raisonnable pourrait suffire. Même chose pour demander un alcootest, une analyse d'haleine sur place ou, comme nous en avons discuté, obtenir des numéros de téléphone.

Le critère du soupçon raisonnable a été approuvé, dans ces affaires, parce que les attentes en matière de vie privée sont faibles. Dans l'arrêt *Hunter c. Southam*, la cour dit que, dans l'établissement d'un équilibre entre le droit à la vie privée et celui de l'État d'enquêter sur des infractions, les fouilles ou les perquisitions fondées sur un soupçon raisonnable se justifient seulement lorsque le droit à la vie privée est faible ou réduit, ce qui tranche spectaculairement sur l'opinion de la Cour suprême dans les arrêts *Vu* et *Spencer*, concernant les métadonnées.

Pas besoin d'être un génie pour se rendre à l'évidence que l'information, dans le cas qui nous occupe, a beaucoup de valeur en matière de vie privée et que le critère ne convient que lorsque sa valeur est faible.

Le président : Je dois vous interrompre ici. Nous devons passer au sénateur Plett.

Le sénateur Plett : Je remercie nos témoins.

If I could, chair, for those of you on the committee who have never toured the Canadian Centre for Child Protection in Winnipeg, I urge you to do so. It is a state-of-the-art facility, and we owe a debt of gratitude to Ms. McDonald and her entire team for what they do. Thank you very much.

In your experience, Ms. McDonald, what do you believe can be done to highlight the dangers of sexting — I think that's the way to pronounce it — sending sexual images, so that individuals don't end up in tragic circumstances?

Ms. McDonald: I think what we're seeing as an agency is the proliferation of this problem. The reality is that young people in most of the cases we deal with are struggling to deal with this. We have a whole generation of children who in many ways do not appreciate the consequences of some of their actions.

Also, looking at this from a child development standpoint and the development of the brain, we see that not happening until into their early twenties. On a daily basis we deal with complaints coming in from kids, typically kids who do not even want an adult around them to know what happened because they are humiliated, pleading with us to figure out some way to manage the damage because of an image that's landed on the Internet. We deal first-hand with those complaints coming in.

That does not even take into consideration some of the cultural considerations. We have kids who come from a variety of backgrounds, which can make their circumstances much worse.

I would say that 4 per cent of the reports come in from kids who have found out who we are and know that our service exists. We hear daily from school resource officers working on the front lines in schools who have to manage this.

To answer the question, this is not just about a legislative response. We believe that Bill C-13 will be important in this regard. I would also note that obviously we recognize that prevention and public education are keys. We see the opportunity to start educating this next generation of kids coming up about the consequences of such behaviour to go a long way in stopping it.

Senator Plett: Ms. St. Germain, you are a lawyer. We have heard, as we hear so many times from our friends, that this is not constitutional and will not pass the constitutional test. I would like your opinion on that.

As well, some have raised concerns about privacy rights, which were raised here again today, being compromised. In your view as legal counsel, does this bill strike the appropriate balance between privacy rights and the safety of Canadians?

Monique St. Germain, General Counsel, Canadian Centre for Child Protection: From everything that our agency has looked at, keeping in mind all the things we deal with, we believe that this bill is constitutional. There has to be a balance struck in

Si vous permettez, monsieur le président, j'encourage vivement tous les membres du comité qui n'ont jamais visité le Centre canadien de protection de l'enfance, à Winnipeg, à le faire. C'est un établissement très moderne, et nous sommes redevables à Mme McDonald et à toute son équipe de ce qu'ils y accomplissent. Merci beaucoup.

D'après vous, madame McDonald, que pouvons-nous faire pour mettre en évidence les dangers du sextage, l'envoi de sextos ou d'images à contenu sexuel, et ainsi empêcher les gens de se retrouver dans le pétrin?

Mme McDonald : Notre organisme constate que le problème se répand. En réalité, la plupart de nos cas sont des jeunes. Toute une génération n'a aucune idée des conséquences éventuelles de ses actions.

De plus, en relation avec le développement de l'enfant et celui du cerveau, le problème ne se manifeste pas avant le début de la vingtaine. Tous les jours, nous recevons des plaintes d'enfants, des enfants qui, habituellement, ne veulent même pas qu'un adulte proche sache ce qui est arrivé parce qu'ils sont humiliés, qui nous implorent de limiter les dégâts, parce qu'une image d'eux a abouti dans l'Internet. Nous répondons directement aux plaintes qui nous parviennent.

Je ne parle même pas des aspects culturels. Ces enfants appartiennent à diverses cultures, ce qui, parfois, risque d'aggraver considérablement leur cas.

Je dirais que 4 p. 100 des signalements nous parviennent d'enfants qui savent qui nous sommes et que notre service existe. Chaque jour, nous sommes en contact avec des policiers éducateurs, qui travaillent en première ligne, dans les écoles, à gérer ce problème.

Pour répondre à la question, cela ne se résume pas à une réponse législative. Nous croyons que le projet de loi C-13 sera important à cet égard. Je ferai aussi remarquer que, manifestement, nous reconnaissons le caractère essentiel de la prévention et de la sensibilisation du public. D'après nous, l'occasion qui nous est offerte de commencer à éduquer la génération montante d'enfants sur les conséquences de ce comportement contribuera beaucoup à y mettre fin.

Le sénateur Plett : Madame St. Germain, vous êtes avocate. Nous avons entendu par nos amis, comme cela arrive si souvent, que cette mesure n'est pas constitutionnelle, qu'elle ne passera pas le test. J'aimerais connaître votre opinion à ce sujet.

De même, certains se sont dits inquiets pour le droit à la vie privée, ce qui a été répété ici même aujourd'hui : ce droit serait mis en péril. En votre qualité de conseillère juridique, trouvez-vous que ce projet de loi concilie bien le droit à la vie privée et la sécurité des Canadiens?

Monique St. Germain, avocate-conseil, Centre canadien de protection de l'enfance : Sous tous les aspects que notre organisme a examinés, sans oublier tous les problèmes dont nous nous occupons, nous croyons que ce projet de loi est

legislation, and I believe this bill has struck the right balance. There is a requirement for people to go before a justice to get these orders; there is some reporting back to justices on many of these orders; and there are strategic ways in terms of information you can obtain through these orders. It seems to us in terms of the stuff we deal with and the things we see that these powers are sorely needed. They have been needed for a very long time, and we are anxious to see this bill come into place.

Senator Jaffer: I have a number of questions, the first one being to Mr. Spratt and Mr. Russomanno. We've all read the *Spencer* case and as lawyers we all have different interpretations of cases. I would appreciate if you would take the time to give us your interpretation and tell us exactly where you think the minister has not interpreted *Spencer,* which you did touch on.

Mr. Russomanno: I will add two main observations and then I'll let Mr. Spratt elaborate.

The first thing relates to the degree of expectation of privacy that attaches to this kind of information. Mr. Spratt touched upon how you have a standard with respect to a warrant, reasonable suspicion being virtually the lowest standard we have compared to "reasonable grounds to believe." The higher the expectation of privacy is, the higher theoretically the standard ought to be.

The court said numerous times, paragraphs 27 and 51, in the *Spencer* decision that there is high expectation of privacy with respect to this information, specifically compared to the dog sniffer cases, as Mr. Spratt referred to, and what kind of expectation of privacy one has for the smell of the contents of their suitcase at an airport.

This is categorically a different kind of information. It is important for the committee to recognize that it's not just the information but what the information tends to reveal about someone — that the Supreme Court goes out of its way to say is one reason that there is a high expectation of privacy, not only the information attached to subscriber data but that which it tends to reveal in a context where people carry out activity where they expect to be anonymous. So there is that high expectation of privacy.

We could spend the entire time today talking about the warrant provisions, but we would be remiss if we did not mention that this bill provides incentives for voluntary disclosure, which is a warrantless search, which is presumptively unreasonable. This is section 810(1) here. We can talk about the low standard, but the more offensive part of the bill is that it provides incentives for ISPs to hand over the stuff, giving them immunity for going flagrantly against what the Supreme Court said, and doing these searches.

constitutionnel. La loi doit trouver le juste milieu, et le projet de loi y parvient. Il exige de s'adresser à un juge de paix pour obtenir les ordonnances; on leur fait rapport sur beaucoup de ces ordonnances; et ces ordonnances permettent, par des moyens stratégiques, d'obtenir l'information recherchée. D'après nous, on avait grandement besoin de ces pouvoirs et depuis très longtemps contre ces problèmes et ces malheurs que nous constatons. Il nous tarde de voir adopter ce projet de loi.

La sénatrice Jaffer : J'ai un certain nombre de questions. La première est pour MM. Spratt et Russomanno. Nous avons tous entendu parler de l'affaire *Spencer* et, en notre qualité d'avocats, nous avons tous un point de vue différent. Je vous serais reconnaissante de bien vouloir prendre le temps de nous faire connaître votre point de vue et nous dire exactement où, d'après vous, le ministre n'a pas interprété l'arrêt *Spencer*, que vous avez effleuré.

M. Russomanno : J'ai deux remarques à faire, puis je laisserai M. Spratt compléter ma réponse.

La première concerne la hauteur des attentes en matière de vie privée pour ce genre d'informations. M. Spratt a parlé d'une norme s'appliquant à un mandat, le soupçon raisonnable étant presque le critère le plus faible que nous possédions, par rapport à celui des motifs raisonnables de croire. Plus l'attente est élevée, plus, en théorie, le critère devrait être rigoureux.

La cour a répété à de nombreuses reprises, dans les paragraphes 27 et 51 de l'arrêt *Spencer*, que les attentes en matière de vie privée pour cette information sont élevées, particulièrement par rapport aux attentes dans les affaires de chiens renifleurs, auxquelles M. Spratt a fait allusion, et pour l'odeur libérée par le contenu des bagages dans une aérogare.

Ici, l'information est catégoriquement différente. Il importe que le comité reconnaisse qu'il ne s'agit pas seulement d'information, mais de ce qu'elle tend à révéler sur quelqu'un. La Cour suprême s'est donné bien du mal pour expliquer la hauteur des attentes en matière de vie privée, qui ne sont pas seulement dues à l'information rattachée aux données des abonnés, mais au fait qu'elles concernent une activité dont les participants requièrent l'anonymat. Les attentes en matière de vie privée sont donc fortes.

Nous pourrions consacrer toute la journée aux dispositions sur les mandats, mais il serait négligent de notre part de ne pas mentionner que le projet de loi encourage la divulgation volontaire, qui est une perquisition ou fouille sans mandat, ce qui, je suppose, n'est pas raisonnable. C'est dans l'article 810(1), ici. Nous pouvons parler de la norme minimale, mais le plus offensant dans le projet de loi est qu'il encourage les fournisseurs d'accès Internet à communiquer l'information, pour obtenir l'immunité pour être allés de manière flagrante à l'encontre de la décision de la Cour suprême et d'avoir effectué ces perquisitions.

Mr. Spratt: We should add that the minister's been quite fond of reading the first half of paragraph 73 of the decision and doesn't always read the last half, which says that the police can't gain new search powers through a combination of a declaratory provision we have in the Criminal Code and through PIPEDA, which is supposed to protect personal privacy. The minister before this committee said that this is no different from when there is a car accident on your street and the police come to your door to ask what you saw. He said that there is no privacy there so why would there be privacy if they are asking the telephone company? The point is that you have no expectation of privacy when you get into a car accident on the street, but according to the Supreme Court you do have expectation of privacy in respect of your data.

When we look at examples like that we have to be careful that we are looking at the proper examples and compare apples to apples, which was not done before this committee.

Senator Jaffer: Ms. McDonald, as you know, since 2010 the Senate has been looking at the issue of cyberbullying. This is not a new issue to us, but it is a highly complicated issue. One of the challenges with the bill is whether we will charge a young person. The testimony before the committee has shown that a child can be a bully, a victim and an observer on the same day, so it just depends on the cycle. It is a huge challenge and you fairly said that this bill is only part of it. We must have a comprehensive approach.

Would you recommend that we recommend to the minister that he set aside funding so that we can have a comprehensive approach to raising awareness because this bill on its own will not stop cyberbullying? We need more. I would like your opinion.

Ms. McDonald: Our agency has been quite vocal on the fact that we're not going to arrest our way out of this problem, nor should we. Public awareness has to be a key component. We have tabled to many parliamentarians the need to support efforts of public awareness to do that.

We also want to note that it's important to take stock of what has happened over the last several years when we look at a number of those high profile cases. Although they may not be the norm, we have to be ready to acknowledge circumstances where things get completely out of control, where parents, educators and everybody else is trying to stop a behaviour that crosses the threshold into criminal activity. For the cases that we have been involved in, we look at the opportunity and this new bill as an important vehicle in certain circumstances.

M. Spratt : Nous devrions ajouter que le ministre a bien aimé lire la première moitié du paragraphe 73 de la décision et qu'il ne lit pas toujours l'autre moitié, dans laquelle on lit que la police ne peut pas obtenir de nouveaux pouvoirs de perquisition ou de fouille en invoquant à la fois une disposition déclarative du Code criminel et la Loi sur la protection des renseignements personnels et les documents électroniques, qui est censée protéger la vie privée. Devant le comité, il a affirmé que ce n'est pas différent d'un accident de voiture qui surviendrait dans votre rue et au sujet duquel la police viendrait sonner à votre porte pour vous demander ce que vous avez vu. Comme il n'est pas question, dans ce cas-là, de protection de la vie privée, pourquoi serait-ce le cas quand la police s'adresse au fournisseur de services de téléphonie? La réponse est qu'on ne s'attend pas à la protection de sa vie privée quand on est victime d'un accident de la route, mais, d'après la Cour suprême, cette attente existe pour nos données.

Il faut se demander, devant de tels exemples, s'ils sont bien choisis et s'ils ne sont pas caricaturaux, ce qui n'a pas été fait devant le comité.

La sénatrice Jaffer : Madame McDonald, comme vous savez, depuis 2010, le Sénat s'intéresse à la cyberintimidation. Pour nous, ce n'est pas un problème nouveau, mais il est très compliqué. L'une des difficultés que pose le projet de loi, c'est la possibilité de porter des accusations contre un jeune. D'après les témoignages que nous avons entendus, un enfant peut être, dans la même journée, tour à tour intimidateur, victime et observateur. Cela dépend seulement du cycle. Cela présente une difficulté importante et vous avez dit, avec raison, que le projet de loi n'est qu'une partie de la réponse. Nous devons adopter une approche globale.

Préconiseriez-vous que nous recommandions au ministre qu'il prévoie du financement pour que nous puissions nous doter d'une approche globale à la sensibilisation, parce que, à lui seul, le projet de loi ne mettra pas fin à la cyberintimidation? Nous avons besoin de plus. J'aimerais connaître votre opinion.

Mme McDonald : Notre organisme a catégoriquement affirmé qu'il n'allait pas entraver la recherche d'une solution à ce problème et qu'il ne devait pas le faire. La sensibilisation du public est essentielle. Nous avons fait connaître à de nombreux parlementaires la nécessité d'appuyer les efforts de sensibilisation du public à cette fin.

Nous voulons aussi faire observer qu'il importait de faire le point sur un certain nombre d'affaires très médiatisées des quelques dernières années. Bien qu'elles ne puissent ne pas être la norme, nous devons être prêts à reconnaître les circonstances dans lesquelles les dérapages se sont produits, dans lesquelles parents, enseignants, tout le monde essaie de mettre fin à un comportement qui devient criminel. Pour les cas qui nous ont été confiés, nous considérons que le projet de loi offre des occasions et des moyens qui peuvent se révéler importants dans certaines circonstances.

I also note as important that it is so easy to separate what we look at as young children under the age of 18. A number of reports and information we receive regularly are from that young adult category — the kids who are 19, 20, and 21 years old whose reputations have been ruined.

It's my understanding that these debates and discussions have been going on for years, but it's been more than 10 years that we have had lawful access discussions, so I think it's time to figure out some of the solutions.

We support this legislation, but to your point, public education and awareness are also key.

Senator Batters: Ms. McDonald, thank you so much for the amazing work you do with your particular group. I'm not sure if you had a chance to read the minister's testimony when he led off this particular study. He complimented the fine work that your organization does and, much like my colleague Senator Plett did today, recommended your centre as one that many people should investigate because it's one to emulate.

Last week, while we were on a constituency week, I was back in my hometown of Regina, Saskatchewan, and I had the opportunity to speak to a Grade 10 class at Campbell Collegiate high school in Regina about what my role in the Senate was and what I do here. I also thought it was the ideal opportunity, when I was speaking to them about the different committees on which I serve, to let them know about the important work we are doing on this particular bill because this is a bill that affects these kinds of kids. I told them a little bit about this bill and also about your website, NeedHelpNow.ca, because that might be the kind of opportunity for a student in that class to hear that. I told them that is somewhere they can go even if they didn't feel comfortable talking to anyone else. After more discussion about that bill, when I was answering questions about various parts during that meeting, I asked the students what they thought about it becoming legislation potentially and whether they thought that the legislation was needed or whether they thought this would be something that could be accomplished with more public education, websites and things like that.

One of the students who responded to that question had been sitting at the front of class, listening attentively, but this was the only thing he said during the one hour I was there. He said: "I really think that we need this as legislation because if there aren't significant consequences, then this kind of thing, people will just keep doing it. It needs to be known that there are significant consequences for this type of activity." I wanted to bring that to your attention.

I also want to give you a bit more of an opportunity. You obviously had a limited time frame with your opening statement to testify about the reasons your organization supports Bill C-13, and you had a little more time when you testified before the House of Commons committee to outline those reasons for your support, but I'm wondering if you could outline that in more detail.

Il importe aussi de noter qu'il est si facile d'oublier les mineurs, les jeunes de moins de 18 ans. Un certain nombre de rapports et de renseignements que nous recevons régulièrement concernent la catégorie de jeunes adultes de 19, 20 et 21 ans, dont la réputation a été ruinée.

D'après ce que j'ai compris, ces débats et ces discussions se poursuivent depuis des années, mais comme on discute depuis plus de 10 ans sur l'accès légal, je pense qu'il est temps d'imaginer des solutions.

Nous appuyons le projet de loi, mais pour répondre à votre question, la sensibilisation et l'éducation du public sont également essentielles.

La sénatrice Batters : Madame McDonald, merci beaucoup pour le travail étonnant de votre groupe. Je ne sais trop si vous avez pu lire le témoignage du ministre, quand il a lancé cette étude particulière. Il a loué l'excellent travail de votre organisation et, plus ou moins comme mon collègue, le sénateur Plett, aujourd'hui, il a recommandé que votre centre soit un modèle à étudier.

La semaine dernière, qui était consacrée à nos circonscriptions, j'étais de retour dans ma ville de Regina où je me suis adressée à une classe de 10e année de l'école secondaire Campbell, pour lui parler de mon rôle et de mes fonctions au Sénat. J'ai aussi pensé que c'était l'occasion idéale, alors que je parlais des différents comités auxquels j'appartiens, pour leur faire connaître le travail important que nous effectuons sur ce projet de loi qui les concerne. Je leur ai aussi parlé de votre site web NeedHelpNow.ca, parce que l'occasion semblait s'y prêter pour cet auditoire. Je leur ai aussi dit qu'ils pouvaient s'adresser à ce site même s'ils ne sentaient pas à l'aise de s'ouvrir à quelqu'un d'autre. Après avoir discuté du projet de loi, alors que je répondais à des questions sur ses différentes dispositions, j'ai demandé aux élèves ce qu'ils pensaient de son éventuelle adoption et s'ils croyaient qu'une telle loi était nécessaire ou qu'on arriverait au même résultat avec plus de sensibilisation du public, plus de sites web et ainsi de suite.

L'un des élèves qui ont répondu à cette question était assis au premier rang de la classe. Il écoutait attentivement, mais c'est la seule chose qu'il a dite pendant cette heure. Il croyait vraiment cette loi nécessaire, parce que si les conséquences n'étaient pas importantes, ce genre de comportement continuerait et qu'il fallait qu'on sache qu'il avait des conséquences importantes. Je tenais à vous le signaler.

Je tiens aussi à vous donner plus de temps de parole. Vous disposiez visiblement de peu de temps pour témoigner dans votre déclaration préliminaire au sujet des raisons pour lesquelles votre organisme appuie le projet de loi C-13 et vous avez disposé d'un peu plus de temps devant le comité de la Chambre pour exposer les motifs de votre appui. Je me demande si vous pouvez les exposer plus en détail.

The Chair: We have limited time.

Ms. McDonald: I just want to say again that we are pleased that this legislation will capture more than just the children under the age of 18. We're pleased that in fact we're not going to be running around charging children with child pornography offences. That is a misplaced charge in many instances, and this is far better suited to do that.

As I mentioned, there has to be some consequence. People need to understand there is a law that does address this and will, in our view, be an important thing that will deter people from committing that crime.

Finally, these conversations about privacy rights are key and we support them as well. Part of the challenge when we're looking at the privacy rights of many children who we would see in child pornography images or in child sexual exploitation images is that they have absolutely no rights as it pertains to what is happening with the distribution of that material. There has to be a balance, and they to be included in the conversation when we are examining important issues related to privacy.

Ms. St. Germain: I think that covers it. It is the deterrent effect that we find very important in this bill in terms of having an appropriate charge to use with young people.

Senator Joyal: I would like to come back to this discussion in relation to the various scales of criteria, depending on the expectation of privacy that is involved.

You made the comparison of somebody with baggage at the airport and the dog comes and smells the bag. Of course, you compare that to the telephone or to the computer. Of course, with a telephone you can trace a person's whereabouts and trace to whom that person has been talking, when, and how many times. There is a lot of data in a telephone that anyone carries these days, and in a computer you have everything.

We have to recognize that by today's standards, those electronic devices store a lot of information that was not available before, and I think it's a caricature to say that when you handle your telephone it's like handling the telephone directory. You just have to watch what Edward Snowden has been disclosing to realize how much information you release with that.

If you establish the principle that the higher the privacy expectation is, the higher the threshold should be of the proof to be made in front of a judge to get such an order, could you explain the highest threshold of proof should be needed to have access to the highest level of expectation of privacy?

Mr. Spratt: Yes. It was the Criminal Lawyers' Association's submissions that were adopted in *Vu*, where we said that computer systems are fastidious record keepers. This is data that is all catalogued, often unwittingly and unknowingly, by the person using the information. Taking into account the decisions

Le président : Nous avons peu de temps.

Mme McDonald : Je tenais simplement à redire que nous sommes heureux que ce projet de loi ne protège pas seulement les enfants de moins de 18 ans. Nous sommes heureux de savoir qu'on ne poursuivra pas les enfants pour les accuser de pornographie juvénile. C'est souvent une accusation injustifiée, et le projet de loi est beaucoup mieux adapté au but recherché.

Comme je l'ai dit, il faut qu'il y ait des conséquences. Les gens doivent comprendre qu'une loi réprime ce comportement, une loi qui, d'après nous, sera un moyen important de dissuasion.

Enfin, nos discussions sur le droit à la vie privée sont essentielles, et nous les appuyons aussi. Une partie de la difficulté que pose le droit à la vie privée de beaucoup d'enfants que nous verrions dans les images de pornographie juvénile et les images montrant l'exploitation sexuelle d'enfants vient du fait qu'ils ne possèdent absolument aucun droit sur la distribution de ces images. Il faut un équilibre et il faut prendre les enfants en considération dans les discussions accompagnant l'examen des enjeux importants du droit à la vie privée.

Mme St. Germain : Je pense que vous avez tout dit. Ce qui nous intéresse dans ce projet de loi et dans le fait d'avoir une infraction qui s'applique aux jeunes, c'est son effet dissuasif.

Le sénateur Joyal : J'aimerais revenir à cette discussion sur les divers critères en fonction de l'attente en matière de vie privée.

Vous avez établi une comparaison avec un individu à l'aéroport et un chien renifleur. Vous comparez cela au téléphone ou à l'ordinateur. De toute évidence, avec un téléphone, on peut suivre les allées et venues d'une personne, retracer les personnes à qui elle a parlé, à quel moment et à quelle fréquence. De nos jours, tout le monde possède un téléphone, et les téléphones renferment énormément d'information. Quant aux ordinateurs, on peut tout trouver là-dedans.

Si l'on se fie aux normes d'aujourd'hui, on doit reconnaître que ces appareils électroniques entreposent beaucoup de données auxquelles on n'avait pas accès auparavant, et je pense que c'est une caricature de dire que de se servir de son téléphone, c'est comme avoir recours à l'annuaire téléphonique. Il suffit de considérer ce qu'Edward Snowden a divulgué pour réaliser tout ce qu'on communique comme information lorsqu'on utilise un téléphone cellulaire.

Si on part du principe que plus l'attente en matière de vie privée est élevée, plus le niveau de preuve requis pour obtenir une ordonnance auprès d'un juge devrait être élevé, pourriez-vous nous expliquer quel devrait être le seuil nécessaire pour qu'on puisse protéger le plus possible la vie privée?

M. Spratt : Oui. Les mémoires de la Criminal Lawyers' Association ont été adoptés dans l'arrêt *Vu*, dans lequel nous affirmons que les systèmes informatiques recueillent des données de façon fastidieuse. Très souvent, on ne sait même pas les données qui y sont entreposées. Si on tient compte des décisions

in the Supreme Court, it's our opinion that the traditional reasonable and probable grounds should be the standard that's inserted. It's an easy change to make: cross out "suspicion" and replace it with "reasonable and probable grounds to believe."

What is sometimes lost is this isn't a question of protecting children or protecting privacy. Both can be accomplished with some minor changes. That's the real tragedy here, especially with respect to children these days who are on the Internet and using digital devices. If anyone needs their privacy protected, it's these children who use these devices and have a much larger digital footprint than any of us will, because they've been on it since they were born. Studies have been done about what you can learn just by having someone's IP address: sites they have commented on; political pages that they've seen on line; who they've talked to; who those people have talked to. This web of information is what necessitates that higher standard of "reasonable and probable grounds to believe," and that is the standard that we use when we search someone's house, when we want to find their location through location tracking. That's the appropriate standard here because it reflects the privacy interest in that information.

We should say that it is not a standard of protection. This isn't proof beyond a reasonable doubt or absolute certainty. This is merely the standard we would suggest that the police need to meet if they were to look into your briefcase. There is a good argument that your online information, even your metadata, which does not include the contents of your communication but includes much other information which can sometimes be more revealing, should be entitled to the same protection as what you might have in your briefcase.

Senator Joyal: In *Spencer*, the Supreme Court understood the technology world in which we live today whereby you can recoup the IP address with, for instance, a credit card number. When you put the two together, you get the whole picture of someone's life. Of course, if you add to that the telephone, you have everything, and it seems to me that the Criminal Code has to reflect the reality of how easy it is now to know everything about anybody.

Mr. Russomanno: Also in *Vu*, the Supreme Court makes an important observation, and I think they refer to it as "digital exhaust," or something along those lines. Our computers and smartphones create a record, a digital footprint, without our intention to create a footprint. Even items that are deleted are not necessarily gone forever. There is a lot of biographical information in there.

It needs to be stressed that getting a warrant is not an onerous requirement. Law enforcement has been operating with this requirement for decades. Getting a warrant is not difficult. I have to say that for this kind of erosion of privacy, I would want to see some demonstrable evidence that a failure to get a warrant or failure to abide by the relatively higher standard of "reasonable grounds to believe" somehow led to victimization here of a child

de la Cour suprême, nous sommes d'avis que les motifs raisonnables et probables devraient être la norme. Il est facile de biffer le terme « soupçons » et de le remplacer par « motifs raisonnables et probables de croire ».

Ce qu'on oublie parfois, c'est que ce n'est pas une question de protéger les enfants ou la vie privée. On peut protéger les deux en apportant des changements mineurs. C'est ce qui est déplorable ici, compte tenu du nombre d'enfants qui naviguent sur Internet et qui utilisent ces appareils aujourd'hui. S'il y a des personnes dont la vie privée doit être protégée, ce sont bien ces enfants qui ont une empreinte numérique beaucoup plus large que la nôtre, étant donné qu'ils baignent là-dedans depuis leur naissance. Des études ont démontré ce qu'on pouvait apprendre seulement par l'adresse IP d'une personne : les sites sur lesquels elle a fait des commentaires; les pages politiques qu'elle a consultées; les personnes à qui elle a parlé; ainsi que les personnes à qui ces personnes ont parlé. Ce réseau d'information exige la norme plus stricte des « motifs raisonnables et probables », et c'est la norme qu'on utilise lorsqu'on fait une perquisition, lorsqu'on veut trouver l'emplacement d'une personne au moyen d'une technologie de localisation. C'est la norme adéquate ici parce qu'elle reflète l'attente en matière de vie privée.

Sachez que ce n'est pas une norme de protection. Il ne s'agit pas d'une preuve hors de tout doute raisonnable ou d'une certitude absolue. C'est simplement la norme qu'utiliserait la police pour fouiller votre mallette. On peut fort bien soutenir que vos informations en ligne, même vos métadonnées, qui n'incluent pas le contenu de vos communications, mais d'autres renseignements qui peuvent parfois être plus révélateurs, devraient bénéficier de la même protection que votre mallette.

Le sénateur Joyal : Dans l'arrêt *Spencer*, la Cour suprême a reconnu l'ère technologique dans laquelle nous vivons aujourd'hui, où il est possible de récupérer l'adresse IP avec un simple numéro de carte de crédit, par exemple. Avec ces deux éléments réunis, on obtient le portrait détaillé de la vie d'une personne. Évidemment, si vous ajoutez à cela le téléphone, vous avez tout, et je considère que le Code criminel doit refléter cette nouvelle réalité, c'est-à-dire la facilité avec laquelle on peut désormais tout savoir sur une personne.

M. Russomanno : Toujours dans l'arrêt *Vu*, la Cour suprême a fait une observation importante. Il était question de « données numériques dérivées » ou de quelque chose du genre. Nos ordinateurs et nos téléphones intelligents laissent une empreinte numérique à notre insu. Même les éléments supprimés ne sont pas nécessairement disparus à jamais. On y retrouve beaucoup de données biographiques.

Il faut souligner que l'obtention d'un mandat n'est pas une exigence contraignante. Les forces policières composent avec cette exigence depuis des décennies. Il n'est pas difficile d'obtenir un mandat de perquisition. En ce qui a trait à l'érosion du droit à la vie privée, j'aimerais avoir des preuves concrètes que l'incapacité d'obtenir un mandat ou de se conformer à la norme plus stricte « des motifs raisonnables de croire » a mené à la victimisation

with respect to cyberbullying. I just don't see that as being the case. I see the drafters responding to something without actually being responsive to any identifiable problem. I think a common thread here, throughout a lot of the crime legislation, is a solution in search of a problem. That's my comment on that.

Senator McIntyre: Thank you all for your presentations. As you know, Bill C-13 includes the "public good" defence. This defence is well-established in Canadian law and is already found in certain sections of the Criminal Code, such as obscenity and voyeurism. As I understand, this defence recognizes that there may be a limited set of circumstances necessary or advantages to religion or morality, the administration of justice, literature or art, the pursuit of science or other aspects of general interest. Under those circumstances, my further understanding is that the police or court officials would be required to share intimate images as part of their disclosure obligations. I would simply have your thoughts on this.

Mr. Spratt: That's nothing new, per se. Quite often, information is shared in disclosure that may be illegal to possess in and of itself.

Senator McIntyre: Yes, because there are certain aspects in the Criminal Code that are already covered with bullying, such as criminal harassment, for example, extortion and so on.

Mr. Spratt: If you look at child pornography cases, as well, the prosecution is often in possession of child pornography images. That's often disclosed to the defence, and there's no suggestion that any crime is being committed through complying with the right to full answer and defence. I wouldn't disagree with your comments at all.

I think that the existing provisions in the Criminal Code arguably cover many of the situations that we're talking about here. In as much as the provisions deal with cyberbullying and updating and making clear some of that law, there may be some quibbles here and there, but it's by far the not very offensive and the least offensive part of this legislation. I don't actually have much to say about the substantive provisions that deal with this bullying.

Senator McIntyre: Ms. St. Germain, do you wish to comment on this?

Ms. St. Germain: On the public good defence?

Senator McIntyre: Yes.

Ms. St. Germain: I have to echo what he said in terms of whether the defence is well-established. In terms of the sharing of information in a criminal context, where there are defence and Crown attorneys possessing it, that's what it would be covered under.

d'un enfant par la cyberintimidation. Ce n'est pas ce que je vois. Je vois que les rédacteurs réagissent à quelque chose sans s'attaquer à un problème précis. Un grand nombre de nos lois destinées à lutter contre la criminalité ont un point en commun : elles sont une solution en quête d'un problème. C'est ce que j'avais à dire là-dessus.

Le sénateur McIntyre : Merci à vous tous pour vos exposés. Comme vous le savez, le projet de loi C-13 renferme la défense « fondée sur le bien public ». Cette défense est bien établie dans le droit canadien, et on la retrouve déjà dans certaines dispositions du Code criminel, notamment celles sur l'obscénité et le voyeurisme. D'après ce que je comprends, cette défense reconnaît qu'il pourrait y avoir des circonstances limitées nécessaires ou favorables à la religion ou à la moralité, à l'administration de la justice, à l'activité scientifique, littéraire ou artistique ou à d'autres sujets d'intérêt général. Dans ces circonstances, à ma connaissance, les policiers ou les fonctionnaires de la cour seraient tenus de communiquer des images intimes en vertu de leurs obligations en matière de divulgation. J'aimerais savoir ce que vous en pensez.

M. Spratt : Cela n'a rien de nouveau. Très souvent, l'information est divulguée, alors qu'il peut être illégal d'être en possession de cette information.

Le sénateur McIntyre : En effet, parce qu'il y a certains aspects du Code criminel qui englobent déjà l'intimidation, comme le harcèlement criminel, l'extorsion et ainsi de suite.

M. Spratt : Si on prend les cas de pornographie juvénile, les procureurs sont souvent en possession d'images de pornographie juvénile. Ces images sont souvent divulguées à la défense, et rien n'indique qu'un crime a été commis lorsqu'on respecte le droit à une défense pleine et entière. Je suis parfaitement d'accord avec vous.

Je pense que les dispositions actuelles du Code criminel couvrent bon nombre des situations dont nous parlons aujourd'hui. Dans la mesure où les dispositions concernent la cyberintimidation et qu'on définit clairement la loi, il pourrait y avoir certains problèmes ici et là, mais c'est de loin la partie la moins offensive de ce projet de loi. En fait, je ne vois aucun inconvénient en ce qui a trait à l'intimidation.

Le sénateur McIntyre : Madame St. Germain, avez-vous quelque chose à dire?

Mme St. Germain : Au sujet de la défense fondée sur le bien public?

Le sénateur McIntyre : Oui.

Mme St. Germain : Je dois faire écho à ce que mon collègue a dit quant à savoir si la défense est bien établie. En ce qui a trait à la communication de renseignements dans un contexte criminel, où les avocats de la défense et les procureurs de la Couronne sont en possession d'informations, on se servirait de cette défense.

The only difference I would point out is that the defence is actually different for child pornography. It's the "legitimate purpose" defence, so it's positioned in a different way because the public good defence was displaced after the *Sharp* decision.

[*Translation*]

Senator Boisvenu: Thank you very much for your testimony. My question is for Mr. Spratt or Mr. Russomanno. You spoke a lot about respecting privacy, and about the fact that this bill does not seem to comply with that law and may even be unconstitutional in that regard. Does your testimony apply as much to the privacy of children as to that of adults?

[*English*]

Mr. Russomanno: As to whether we speak to the privacy of children versus that of adults, I would echo Mr. Spratt's comments about the privacy of children being just as important.

Senator Boisvenu: So it's both adults and kids.

Mr. Russomanno: Absolutely.

[*Translation*]

Senator Boisvenu: What do you think about parents who force their children to disclose the information on their computers so that they can check it? When parents have easy access to the information on their children's computers, do you feel that the parents are violating the children's privacy?

[*English*]

Mr. Russomanno: I think we have to be careful when we talk about this right to privacy because, in the language of the Charter, when we talk about a privacy right, it's against the government; but in the everyday sense, yes, a child's privacy is being infringed upon when the parent takes a look at what's in their computer. However, in many cases, it could be a valid parenting exercise.

Mr. Spratt: I might be the law in my house when it comes to me and my children, but the Charter doesn't apply to my interactions with my children. I'm not violating their right to privacy under section 8.

[*Translation*]

Senator Boisvenu: I would like to ask a final question. We know how easy it is for sexual predators to enter into a relationship with children now. It is also in a parenting situation where the supervision leaves something to be desired and the child is alone with the computer. What takes priority then? Do we prioritize the protection of the child from a predator getting into the child's personal life with ease, or do we have to protect the private information belonging to that sexual predator

Toutefois, la situation est différente dans le cas de la pornographie juvénile. On parle plutôt d'une défense « fondée sur le but légitime », qui a remplacé la défense fondée sur le bien public à la suite de l'arrêt *Sharp*.

[*Français*]

Le sénateur Boisvenu : Merci beaucoup pour vos témoignages. Ma question s'adresse à M. Spratt ou à M. Russomanno. Vous avez beaucoup parlé du respect de la vie privée et du fait que ce projet de loi semble ne pas respecter cette loi et qu'il serait même anticonstitutionnel à cet égard. Vous parlez aussi bien de la vie privée des enfants que des adultes dans votre témoignage?

[*Traduction*]

M. Russomanno : En ce qui concerne la vie privée des enfants par rapport à celle des adultes, j'abonde dans le même sens que M. Spratt, c'est-à-dire que la vie privée des enfants est tout aussi importante.

Le sénateur Boisvenu : Par conséquent, on vise autant la protection de la vie privée des adultes que celle des enfants.

M. Russomanno : Absolument.

[*Français*]

Le sénateur Boisvenu : Que pensez-vous des parents qui obligent leur enfant à rendre disponible l'information sur leur ordinateur pour effectuer des validations? Lorsque les parents ont accès facilement à l'information des ordinateurs de leur enfant, est-ce que, selon vous, les parents violent la vie privée des enfants?

[*Traduction*]

M. Russomanno : Je pense qu'il faut faire attention lorsqu'il est question de ce droit à la vie privée parce que, dans le contexte de la Charte, lorsqu'on parle du droit à la vie privée, c'est contre le gouvernement : mais au sens usuel du terme, oui, lorsqu'un parent vérifie dans l'ordinateur de son enfant, il porte atteinte à sa vie privée. Toutefois, dans bien des cas, c'est un exercice parental valide.

M. Spratt : Je peux établir mes règles dans ma maison lorsqu'il s'agit de moi et de mes enfants, mais la Charte ne s'applique pas à mes interactions avec mes enfants. Je n'enfreins pas leur droit à la vie privée en vertu de l'article 8.

[*Français*]

Le sénateur Boisvenu : J'aimerais poser une dernière question. On connaît la facilité avec laquelle les prédateurs sexuels entrent maintenant en interrelation avec les enfants, et c'est souvent aussi dans un contexte parental où l'encadrement laisse à désirer et où l'enfant est donc seul avec l'ordinateur. Que doit-on alors privilégier? Faut-il d'abord privilégier la protection de l'enfant par rapport au prédateur qui entre facilement dans sa vie personnelle ou doit-on protéger les renseignements privés qui

who has established contact with the child? When we talk about checks and balances, which aspect must be given priority? Must we not first give the priority to protecting our children?

[*English*]

Mr. Russomanno: I would say that in the circumstances that you just outlined it's not necessarily a matter of one versus the other, which is why I opened my comments by saying that Charter rights protect not only those that commit crimes but all of us. I would say that there is an obvious importance to protecting the online privacy of children that are vulnerable to being preyed upon by child predators. There's obviously a valid public safety issue there, but I have to echo my earlier comment that I don't know that there has been a demonstrated need to actually weaken all of our privacy protections in order to protect this group of people.

[*Translation*]

Senator Dagenais: My thanks to our guests.

My first question goes to Ms. McDonald. Clause 24 of the bill allows the court to make a restitution order against an accused found guilty of the offence of distributing intimate images, if the person affected by the offence incurs expenses to remove the images from the Internet or other digital network. In your opinion, could that restitution order also allow for compensation for moral and psychological damages?

[*English*]

Ms. McDonald: I defer to my colleague, Ms. St. Germain. We're just trying to find that section right now.

Ms. St. Germain: Clause 24, you said?

[*Translation*]

Senator Dagenais: Yes, clause 24.

[*English*]

Ms. St. Germain: Could you repeat the question?

[*Translation*]

Senator Dagenais: There is a provision for compensation when a person is found guilty of the offence. At that point, it may sometimes be the case that the victim has incurred expenses in order to have the images removed from the Internet or digital network. Could there not also be a provision for compensation for moral and psychological damages, for which the accused would be responsible?

appartiennent au prédateur sexuel qui est entré en contact avec cet enfant? Lorsqu'on parle de freins et de contrepoids, à quel élément doit-on accorder la priorité? Ne doit-on pas d'abord accorder la priorité à la protection de nos enfants?

[*Traduction*]

M. Russomanno : Je dirais que dans les circonstances que vous venez tout juste d'exposer, il n'est pas forcément question de protéger la vie privée d'une personne au détriment d'une autre, c'est pourquoi j'ai commencé en disant que les droits garantis par la Charte protègent non seulement ceux qui commettent les crimes, mais aussi tout le reste de la population. De toute évidence, il est important de protéger la vie privée en ligne des enfants vulnérables qui peuvent devenir des proies faciles pour des prédateurs sexuels. Bien entendu, il y a une question de sécurité publique valide ici, mais comme je l'ai dit plus tôt, je m'interroge sur la nécessité d'affaiblir notre protection de la vie privée afin de protéger ce groupe de gens.

[*Français*]

Le sénateur Dagenais : Merci à nos invités.

Ma question s'adresse à Mme McDonald. L'article 24 du projet de loi permet au tribunal de rendre une ordonnance de dédommagement contre l'accusé reconnu coupable de l'infraction de distribution d'images intimes si la personne touchée a engagé des dépenses liées au retrait de ces images, soit sur un site Internet ou sur tout autre réseau numérique. Selon vous, cette ordonnance pourrait-elle également prévoir un dédommagement pour des dommages moraux et psychologiques?

[*Traduction*]

Mme McDonald : Je vais m'en remettre à ma collègue, Mme St. Germain. Nous essayons de trouver cet article.

Mme St. Germain : L'article 24, vous avez dit?

[*Français*]

Le sénateur Dagenais : Oui, il s'agit de l'article 24.

[*Traduction*]

Mme St. Germain : Pourriez-vous répéter la question?

[*Français*]

Le sénateur Dagenais : Il est prévu un dédommagement lorsqu'une personne est reconnue coupable de l'infraction. À ce moment-là, il se peut que, dans certains cas, la victime ait engagé des frais pour retirer les images du site Internet ou d'un réseau numérique. Ne pourrait-on pas aussi prévoir un dédommagement pour des dommages moraux et psychologiques et en tenir responsable l'accusé?

[*English*]

Ms. St. Germain: I think that there should be some damages for that, but we're looking at the bill the way it has been drafted in terms of damages and different opportunities that there might be for a victim to recover. There are obviously civil matters that people could proceed with as well. Definitely, removing the images from the Internet, to the extent that they're readily ascertainable, is what this is trying to say.

Ms. McDonald: If I may add to that, we've been participating in some consultation on the Victim Bill of Rights. I think restitution is another issue that we're looking at. One of the things that our agency deals with when we're dealing with, particularly, victims of child pornography, is that their past is really their present. So we will have victims who have grown up in a series of child abuse. Years after, let's say, the offender has been arrested, the images are still propagating online. Often these young adults have significant challenges and problems carrying on. So we see a lot of issues surrounding the need for therapeutic services that go on for many years.

[*Translation*]

Senator Dagenais: So you would be in favour of compensation for those people if they have to incur expenses, because of the moral and physiological damages they have suffered?

[*English*]

Ms. McDonald: Ideally, if it were possible, it certainly would be something that our agency would support.

[*Translation*]

Senator Dagenais: We can always hope for an ideal world. Thank you, Madam.

[*English*]

Senator Baker: I appreciate the evidence given to us today and it's very clear what your positions are. Perhaps I could get some clarity.

Mr. Spratt and Mr. Russomanno, even without this bill, would you not agree that perhaps we should look again at the present provisions of PIPEDA and the Criminal Code regarding production orders in which this information we're referencing today can be disclosed to any police investigation under a present production order? Even without this bill, perhaps we should re-examine, given your evidence, present provisions in the code that allow such information to be divulged.

Mr. Spratt: I think there are two options: Either the provisions in PIPEDA could be strengthened to reflect the protection of personal information, or the title of the act could be changed to reflect the reality of what it allows.

[*Traduction*]

Mme St. Germain : Je pense qu'il devrait y avoir un dédommagement pour cela, mais nous nous penchons sur le projet de loi actuel ainsi que sur les dommages et intérêts et les différentes possibilités pour la victime de récupérer ces sommes. Évidemment, elle pourrait intenter des poursuites civiles. Essentiellement, retirer les images d'Internet, dans la mesure où elles sont facilement déterminables, est ce que prévoit ce projet de loi.

Mme McDonald : Si je puis me permettre, nous avons participé aux consultations entourant la Charte des droits des victimes. Le dédommagement est un autre aspect que nous examinons. L'une des choses dont notre organisme doit tenir compte lorsqu'il traite avec des victimes de pornographie juvénile, particulièrement, c'est que leur passé est toujours présent. Par conséquent, nous aurons affaire à des victimes qui ont subi des abus durant leur enfance. Plusieurs années plus tard, le contrevenant a été arrêté, mais les images sont toujours en ligne. Souvent, ces jeunes adultes sont aux prises avec de graves problèmes. Bon nombre d'entre eux doivent recevoir des services thérapeutiques pendant de nombreuses années.

[*Français*]

Le sénateur Dagenais : Vous seriez donc d'accord pour qu'il y ait un dédommagement pour ces personnes si elles doivent engager des frais, parce qu'elles ont subi des dommages moraux et psychologiques?

[*Traduction*]

Mme McDonald : Idéalement, si c'était possible, ce serait certainement quelque chose que notre organisme appuierait.

[*Français*]

Le sénateur Dagenais : On peut toujours attendre un monde idéal. Je vous remercie, madame.

[*Traduction*]

Le sénateur Baker : J'apprécie vos témoignages, et vos positions sont très claires. J'aurais toutefois besoin d'une précision.

Messieurs Spratt et Russomanno, même sans ce projet de loi, ne pensez-vous pas qu'il serait nécessaire qu'on se penche de nouveau sur les dispositions actuelles de la LPRPDE et du Code criminel concernant les ordonnances de communication en vertu desquelles cette information peut être divulguée à la police dans le cadre d'une enquête? Même sans ce projet de loi, à la lumière de votre témoignage, nous devrions peut-être réexaminer les dispositions actuelles du Code criminel qui permettent de divulguer de tels renseignements.

M. Spratt : Je pense que nous avons deux options : renforcer les dispositions de la LPRPDE pour refléter la protection des renseignements personnels ou modifier le titre pour refléter ce que permet la loi.

Senator McIntyre: My question is directed to Mr. Spratt and Mr. Russomanno. As you know, certain aspects of cyberbullying are already criminalized, such as criminal harassment, uttering threats, intimidation and extortion. What is not criminalized is what's contained in Bill C-13, in other words, the distribution of non-consensual images. As criminal defence lawyers, have you had any experience with those offences that deal with cyberbullying? What were the results?

Mr. Russomanno: I have not had experience specifically with cyberbullying. I have had a lot of experience defending cases of criminal harassment and similar cases but not specifically within the cyberbullying context. It's not something that I see very often.

Mr. Spratt: I've not had experience dealing with the dissemination of intimate or personal images, as would be covered under this bill. I think most criminal defence lawyers who have represented anyone charged with harassment, threats, intimidation, or any youthful offences have dealt with the interception of online activity and inappropriate communications. In almost every youth court case that we see, we have Facebook messages, Twitter messages, and social media commentary between accused persons and witnesses, and witnesses and accused persons. It definitely is something that can be dealt with under the Criminal Code.

The fact that this bill specifically deals with that other aspect, even if it's already criminalizing other contexts, there is nothing wrong with providing additional clarity for that intimate image section.

Senator Jaffer: My question is around the intimate images. Do you think this will help, especially in youth court? My concern is that it's youth against youth. Some cases involve adults but often it is youth against youth. Do you think this is an appropriate way to deal with young people? You both have experience in youth court.

Mr. Spratt: The precision in which the conduct is defined in the bill is helpful. It's already covered under some sections that we have, but it is helpful.

In dealing with youth specifically, something we haven't talked about today, which is a concern of some organizations and of our organization as well, is the term "reckless" found in the bill. Especially when we're dealing with youthful individuals, the term "reckless" might capture a lot of action that wouldn't otherwise be captured by adults who might act in a less youthful way. As we know, youth can be more reckless on occasion. With that reckless standard, there is a chance that this bill might actually more broadly apply to youthful activity than to adult activity. That reckless standard and the lowering of the intense standard in that section might merit some consideration as well.

Le sénateur McIntyre : Ma question s'adresse à MM. Spratt et Russomanno. Comme vous le savez, certains aspects de la cyberintimidation sont déjà criminalisés, tels que le harcèlement criminel, la profération de menaces, l'intimidation et l'extorsion. Ce qui n'est pas criminalisé est ce que l'on trouve dans le projet de loi C-13, autrement dit, la distribution non consensuelle d'images. À titre d'avocat de la défense, quelle a été votre expérience relativement à ces infractions qui traitent de la cyberintimidation? Quelle a été l'issue des accusations?

M. Russomanno : Je n'ai pas d'expérience en matière de cyberintimidation. J'ai défendu de nombreuses causes de harcèlement criminel et d'autres causes semblables, mais pas précisément dans le contexte de la cyberintimidation. C'est quelque chose que je ne vois pas très souvent.

M. Spratt : Je n'ai pas encore traité de la diffusion d'images intimes ou personnelles, comme le prévoit le projet de loi. Je pense que la plupart des avocats de la défense qui ont représenté une personne accusée de harcèlement, de profération de menaces, d'intimidation ou de toute autre infraction impliquant des jeunes ont dû se pencher sur l'interception d'activités en ligne et les communications inappropriées. Dans presque toutes les causes devant les tribunaux pour jeunes que nous voyons, il est question de messages Facebook, de messages Twitter et d'échanges sur les réseaux sociaux entre les personnes accusées et les témoins, et vice versa. Ce sont assurément des affaires qui peuvent être traitées sous le régime du Code criminel.

Le fait que ce projet de loi concerne précisément cet autre aspect, même si c'est déjà criminalisé dans d'autres contextes, il n'y a rien de mal à clarifier davantage cette disposition sur la distribution d'images intimes.

La sénatrice Jaffer : Ma question porte sur les images intimes. Croyez-vous que ce projet de loi sera utile, particulièrement dans les tribunaux pour adolescents? Ce qui m'inquiète, c'est que ce sont des enfants contre d'autres enfants. Certains cas impliquent des adultes, mais on retrouve surtout des enfants. Selon vous, est-ce la meilleure façon de traiter les adolescents? Vous avez tous les deux de l'expérience devant les tribunaux pour jeunes.

M. Spratt : Le niveau de précision dans la façon de définir la conduite dans le projet de loi est utile. Cela tombe déjà sous le coup d'autres articles, mais cette précision est utile.

Lorsqu'il est question des jeunes en particulier, ce qui préoccupe certaines organisations, y compris la nôtre, c'est la notion d'insouciance qui se trouve dans le projet de loi. Lorsqu'on traite avec des jeunes individus, la notion d'insouciance pourrait englober beaucoup d'actions qui nous échapperaient s'il s'agissait d'adultes. Comme nous le savons, les jeunes peuvent être plus insouciants à l'occasion. Cela dit, il est possible que ce projet de loi s'applique davantage aux activités des jeunes qu'aux activités des adultes. Cette notion d'insouciance et l'assouplissement de la norme dans cet article méritent qu'on s'y attarde également.

Senator Batters: When our committee last met on this bill on November 5, Norman Wong, Counsel for Criminal Law Policy, Justice Canada, told us about a federal-provincial-territorial ministers committee called the Coordinating Committee of Senior Officials Cybercrime Working Group. They published a report, which you may be familiar with, called "Cyberbullying and the Non-consensual Distribution of Intimate Images." For that working group, Mr. Wong said:

> Following the tragic death of Rehtaeh Parsons, which followed only a few months after the Amanda Todd situation, all FPT ministers responsible for justice and public safety were engaged on the issue of cyberbullying. They asked the working group to look at this issue.
>
> We met for a number of days to study this. Also, the working group is composed of policy people, prosecutors and police from across all Canadian jurisdictions.

The Chair: Can we have the question please?

Senator Batters: He continued:

> There were approximately 30 people who worked on that, all very experienced practitioners in this area of the law.

The fourth recommendation of their report called on the government to give the police the investigative tools to investigate cyberbullying and other online crime. Mr. Spratt, could you tell us why, in your view, those 30 experts on that working group were wrong in calling on the government to include these kinds of investigative tools in cyberbullying legislation?

Mr. Spratt: Investigators need tools to investigate these crimes. Unfortunately, the tools suggested in this bill are unconstitutional. They need constitutional tools to properly investigate crimes. The Supreme Court said high expectation of privacy for high privacy value. The Supreme Court said reasonable suspicion only for low privacy value. There is no way to square that circle. Don't give them a tool that's going to be struck down in a year or two.

Senator Batters: You're view is split and study.

The Chair: Witnesses, thank you all. Your appearance and testimony are much appreciated by the committee.

La sénatrice Batters : Lorsque notre comité s'est réuni le 5 novembre dernier dans le cadre de son étude de ce projet de loi, Norman Wong, avocat à la Section de la politique en matière de droit pénal au ministère de la Justice, nous a parlé du Groupe de travail sur la cybercriminalité du Comité de coordination des hauts fonctionnaires, auquel siègent des ministres fédéraux-provinciaux-territoriaux. Ce groupe a publié un rapport, que vous connaissez sûrement, intitulé *Cyberintimidation et distribution non consensuelle d'images intimes*. Dans ce contexte, M. Wong a déclaré :

> Après la mort tragique de Rehtaeh Parsons, qui est survenue quelques mois seulement après celle d'Amanda Todd, tous les ministres fédéraux-provinciaux-territoriaux responsables de la Justice et de la Sécurité publique se sont penchés sur la question de la cyberintimidation. Ils ont demandé au groupe de travail d'examiner la question.
>
> Nous nous sommes réunis plusieurs jours pour étudier la question. En outre, le groupe de travail se compose de décideurs, d'avocats et d'agents de police provenant de l'ensemble des provinces et des territoires canadiens.

Le président : Pouvons-nous avoir la question, s'il vous plaît?

La sénatrice Batters : Il a poursuivi :

> Quelque 30 personnes ont mis la main à la pâte, tous des professionnels chevronnés de ce domaine du droit.

La quatrième recommandation du rapport consistait à demander au gouvernement d'accorder aux services de police les outils d'enquête nécessaires pour mener les enquêtes sur la cyberintimidation et d'autres crimes en ligne. Monsieur Spratt, pourriez-vous nous dire pourquoi, à votre avis, ces 30 experts du groupe de travail avaient tort de demander au gouvernement d'inclure ce genre d'outils d'enquête dans une mesure législative sur la cybercriminalité?

M. Spratt : Les enquêteurs ont besoin d'outils pour mener des enquêtes sur ces crimes. Malheureusement, les outils proposés dans le projet de loi sont inconstitutionnels. Ils ont besoin d'outils constitutionnels pour mener adéquatement des enquêtes sur ces crimes. La Cour suprême a indiqué que les attentes en matière de protection de la vie privée sont élevées dans les cas où les intérêts en matière de vie privée sont élevés. La Cour suprême a indiqué que le soupçon raisonnable devait s'appliquer uniquement aux situations où les intérêts en matière de vie privée sont faibles. C'est incontournable. Ne leur donnez pas un outil qui sera invalidé dans un an ou deux.

La sénatrice Batters : Vous préconisez de scinder le projet de loi et de l'examiner.

Le président : Merci à tous les témoins. Le comité vous est très reconnaissant d'être venus et d'avoir témoigné.

For our second panel today, I would like to welcome Andrea Slane, Associate Professor, University of Ontario Institute of Technology; and Michael Geist, Law Professor, University of Ottawa.

Professor Slane, I believe you will begin with the opening remarks, followed by Professor Geist.

Andrea Slane, Associate Professor, University of Ontario Institute of Technology, as an individual: My research and a lot of my policy-oriented work has been in two areas. One is online child exploitation and how to best address those problems, and the other has been with the appropriate scope of voluntary cooperation with police investigations, especially on the part of Internet service providers. It does span both aspects of this bill. I have struggled a lot with how to bring those things together. That's why I'm here today, how to honour those two objectives.

The bill isn't entirely integrated. It is something that deals with two different types of problems, but insofar as I have tried to bring those things together, I am happy to offer my views.

There are many aspects of the bill that I support, including the new offence on non-consensual distribution of intimate images. I will not spend a lot of time talking about that, although I do welcome questions.

There are important tools in this bill that need to be implemented, but I would agree with some of the comments made by the previous panel about things that need to be tweaked in order to make those tools appropriate to the privacy protection of all of us that is set out in the Charter.

I also applaud the drafters for taking out the most controversial aspects of the last iteration of the bill, and some of the iterations beforehand, regarding warrantless access. This is an improved bill, though I do still have some problems.

I only want to focus on one thing since my introductory comments are supposed to short. I want to reiterate some of the things that were said in the previous panel about transmission data, the inappropriateness of the reasonable suspicion standard for the production orders and the transmission data recorder warrant for transmission data specifically.

There has been an increasing amount of testimony in other places about the sensitivity that transmission data reveals about people's lives, especially insofar as there's a kind of fallacy that the government has been putting forward about this and that it is somehow less sensitive than content. There are a couple of

Nous passons à notre deuxième groupe d'experts. Nous accueillons Mme Andrea Slane, qui est professeure agrégée à l'Institut universitaire de technologie de l'Ontario, et M. Michael Geist, qui est professeur de droit à l'Université d'Ottawa.

Madame Slane, vous serez la première à présenter votre exposé, puis ce sera au tour de M. Geist.

Andrea Slane, professeure agrégée, Institut universitaire de technologie de l'Ontario, à titre personnel : Ma recherche et une bonne partie de mes travaux en matière de politiques portent sur deux aspects. Le premier est l'exploitation des enfants sur Internet et les meilleures façons de s'attaquer à ces problèmes, et l'autre est la détermination de la portée adéquate relativement à la collaboration volontaire dans le cadre d'enquêtes policières, en particulier pour ce qui est des fournisseurs de services Internet. Cela touche donc aux deux aspects du projet de loi. J'ai beaucoup réfléchi à la façon d'établir un lien entre ces deux choses. Voilà pourquoi je suis ici aujourd'hui; je veux parler de la façon d'atteindre ces deux objectifs.

Le projet de loi n'est pas entièrement intégré. Il traite de deux types de problèmes distincts, mais étant donné que j'ai essayé d'établir un lien entre ces deux aspects, je suis heureuse de vous présenter mes observations.

J'appuie beaucoup d'éléments du projet de loi, notamment la nouvelle infraction relative à la distribution non consensuelle d'images intimes. Je ne consacrerai pas beaucoup de temps à en parler, mais c'est avec plaisir que je répondrai aux questions.

Le projet de loi comporte d'importants outils qui doivent être mis en œuvre, mais je serais d'accord sur certains commentaires présentés par les gens du groupe d'experts précédent voulant que certaines choses doivent être modifiées afin que ces outils respectent le droit de tous les Canadiens à la protection de la vie privée, comme énoncé dans la Charte.

Je félicite aussi les rédacteurs d'avoir retiré les aspects les plus controversés de la dernière version du projet de loi — et de versions antérieures — concernant l'accès sans mandat. Il s'agit d'un projet de loi amélioré, même si j'ai toujours quelques réserves.

Étant donné que ma déclaration préliminaire est censée être courte, je vais me concentrer sur un seul aspect. Je tiens à reprendre certains propos des témoins précédents concernant les données de transmission et le caractère inapproprié de la norme des soupçons raisonnables pour les ordonnances de communication et pour les mandats relatifs aux enregistreurs de données de transmission en particulier.

Sur d'autres tribunes, de plus en plus de témoignages font état de la nature délicate des renseignements que les données de transmission permettent de révéler sur la vie des gens, surtout étant donné que le gouvernement a véhiculé certaines faussetés à cet égard en disant que c'était en quelque sorte de nature moins

problems with the logic that says that if it's less sensitive than content, it deserves a lesser level of scrutiny to meet that threshold.

One problem is that it isn't necessarily less sensitive than content. I want to quote from Professor Edward Felten, a professor of computer science and public affairs at Princeton University. When I submitted to this committee in May, along with Professor Lisa Austin from University of Toronto, we gave you the full testimony that he gave before a U.S. Senate committee, much like this one, though it was focused on foreign intelligence surveillance there.

He says:

> It is no longer safe to assume that this 'summary' or 'non-content' information is less revealing or less sensitive than the content it describes . . . Just by using new technologies such as smart phones and social media, we leave rich and revealing trails of metadata as we move through daily life. Many details of our lives can be gleaned by examining those trails.

It's important to recognize that in the past we may have thought of there being a distinction between content, which all of us agree is highly sensitive and therefore requires a lot of privacy protection, and the information that surrounds digital communications as they travel through cyberspace and across our various networks.

It's also important to think about what the Canadian public expects from this type of information. It was raised in the last panel about the National Security Agency in the United States and the revelations we found on CSEC's testing on that type of data mining they're able to do and analysis they're able to do of metadata. Just this past January, the news broke that there was a test done via a Canadian airport's Wi-Fi and a lot of people were deeply upset. It was not content that was being examined then; it was just metadata. Nonetheless, it shows that the Canadian public also believes the way that their information travels across a network and the Internet is something they would consider private and would therefore require the same standard of that type of information as they do of content data.

My last point on this — and again I welcome questions not just about this but other aspects of the bill that I don't have time to address in these introductory remarks — is that you cannot base anything having to do with digital communication technologies on what we've done before for telephones, an analog technology. It seems completely inappropriate to think that because a certain

délicate que le contenu. La logique selon laquelle l'atteinte de ce seuil ne requiert pas une aussi grande surveillance étant donné que c'est de nature moins délicate que le contenu pose deux ou trois problèmes.

Un des problèmes, c'est que ce n'est pas nécessairement de nature moins délicate que le contenu. J'aimerais citer le professeur Edward Felten, un professeur de sciences informatiques et d'affaires publiques à l'Université Princeton. Dans le mémoire que j'ai présenté à ce comité au mois de mai, en collaboration avec la professeure Lisa Austin, de l'Université de Toronto, nous vous avons fourni le témoignage qu'il a livré devant un comité sénatorial américain semblable à celui-ci, même s'il était question de la surveillance du renseignement étranger.

Il a dit ce qui suit :

> On ne peut plus présupposer sans se tromper que ces renseignements « sommaires » ou « sans contenu » sont moins révélateurs ou moins sensibles que le contenu qu'ils décrivent. Ne serait-ce qu'en utilisant de nouvelles technologies comme les téléphones multifonctions et les médias sociaux, nous laissons quotidiennement derrière nous une mine de métadonnées révélatrices et riches en renseignements. Bien des détails sur nos vies personnelles peuvent être obtenus en examinant ces traces.

Il est important de reconnaître que dans le passé, nous avons peut-être pensé qu'il y avait une distinction à faire entre le contenu — qui, nous en convenons tous, est de nature très délicate et exige par conséquent une grande protection en matière de vie privée — et l'information liée aux communications numériques qui est transmise dans le cyberespace et divers réseaux.

Il est aussi important de penser aux attentes du public canadien à l'égard de ce genre d'information. La question a été soulevée par le dernier groupe d'experts lorsqu'il a été question de la National Security Agency, aux États-Unis, et des révélations sur les tests menés par le CSTC par rapport à l'exploration de données et à l'analyse des métadonnées. En janvier dernier, les médias ont révélé que le réseau sans fil d'un aéroport canadien avait été utilisé pour faire des tests, ce que beaucoup de personnes ont été profondément bouleversées d'apprendre. À ce moment-là, on n'a pas examiné le contenu, mais simplement les métadonnées. Quoi qu'il en soit, cela démontre que le public canadien considère également que la transmission de leurs informations sur un réseau et sur Internet est du domaine privé et que par conséquent, les normes relatives à ce genre d'informations devraient être identiques à celles des données de contenu.

Mon dernier point à ce sujet — et encore une fois, je suis prête à répondre aux questions, pas seulement sur ce point, mais aussi sur d'autres aspects du projet de loi dont je n'ai pas eu le temps de parler pendant cet exposé —, c'est qu'aucune mesure liée aux technologies de communication numérique ne peut être fondée sur ce que nous avons fait auparavant par rapport au téléphone,

standard applies to telephone number recorders or has applied in the past to telephones that used to be land lines, it would translate in any kind of direct way to current technologies.

I'll stop there.

Michael Geist, Law Professor, University of Ottawa, as an individual: Good afternoon. My name is Michael Geist, a law professor at the University of Ottawa, where I hold the Canada Research Chair in Internet and E-commerce Law. I appear today in a personal capacity representing only my own views.

Given the limited time, I would like to focus on three privacy-related issues that you have already heard about today: the immunity for voluntary disclosure provision, the low threshold for transmission data warrants, and the absence of reporting and disclosure requirements.

I should start by first emphasizing that criticism of lawful access legislation doesn't mean opposition to ensuring that our law enforcement agencies have the tools they need to address crime in the online environment. As Carol Todd, Amanda Todd's mother, told the House of Commons committee that studied Bill C-13, "we should not have to choose between our privacy and our safety." Similarly, Sue O'Sullivan, the Federal Ombudsman for Victims of Crime, told the committee that victims were split on the bill precisely because of the privacy concerns arising out of Bill C-13.

Let me focus on these three issues that I promised you.

First, on immunity for voluntary disclosure, I think it should be viewed within the context of five facts.

First, as you heard earlier, the Supreme Court of Canada's *Spencer* decision confirms that there is a reasonable expectation of privacy in subscriber information and clearly indicates that, absent exigent circumstances, disclosures should involve a warrant.

Second, pre-*Spencer* intermediaries disclose personal information on a voluntary basis without a warrant with shocking frequency. The revelation earlier this year of 1.2 million requests to telecom companies for customer information in 2011 affecting 750,000 user accounts provides a hint of the privacy impact of voluntary disclosures.

qui est une technologie analogique. Il semble totalement inapproprié de penser qu'une norme quelconque qui s'applique aux enregistreurs de numéros de téléphone ou qui s'appliquait auparavant à des services téléphoniques par ligne terrestre peut s'appliquer directement aux technologies actuelles.

Je vais arrêter ici.

Michael Geist, professeur de droit, Université d'Ottawa, à titre personnel : Bonjour, je m'appelle Michael Geist. Je suis professeur en droit à l'Université d'Ottawa. Je suis titulaire de la chaire de recherche du Canada en droit d'Internet et du commerce électronique. Aujourd'hui, je témoigne à titre personnel et je vous présenterai mes propres points de vue.

Puisque j'ai peu de temps, j'aimerais me concentrer sur trois enjeux liés à la protection de la vie privée dont vous avez déjà entendu parler aujourd'hui : la disposition sur l'immunité en cas de communication volontaire, le faible seuil concernant le mandat relatif aux données de transmission et l'absence d'exigences en matière de présentation de rapports et de divulgation.

Je veux commencer en soulignant que le fait de critiquer les projets de loi sur l'accès légal ne signifie pas qu'on est contre l'idée de s'assurer que les organismes d'application de la loi ont les outils dont ils ont besoin pour lutter contre la criminalité en ligne. Comme Mme Carol Todd — la mère d'Amanda Todd — l'a indiqué devant le comité de la Chambre des communes qui s'est penché sur le projet de loi C-13 : « Nous ne devrions pas être obligés de choisir entre la vie privée et la sécurité. » De même, Mme Sue O'Sullivan, l'ombudsman fédérale pour les victimes de crime, a dit au comité que les victimes étaient divisées au sujet du projet de loi en raison des préoccupations en matière de protection de la vie privée que soulève le projet de loi C-13.

Permettez-moi de me concentrer sur les trois enjeux dont j'ai promis de parler.

Premièrement, en ce qui concerne l'immunité en cas de communication volontaire, je pense que cela doit être examiné à la lumière de cinq faits.

Premièrement, comme vous l'avez entendu plus tôt, dans la décision *Spencer*, la Cour suprême du Canada confirme qu'il existe des attentes raisonnables en matière de vie privée pour ce qui est des données sur les abonnés et indique clairement qu'à moins de circonstances exceptionnelles, la communication devrait faire l'objet d'un mandat.

Deuxièmement, avant la décision *Spencer*, les intermédiaires divulguaient volontairement des renseignements personnels sans mandat à une fréquence troublante. La révélation, plus tôt cette année, du fait que 1,2 million de demandes ont été présentées aux entreprises de télécommunications en 2011 pour la communication des renseignements des clients — touchant ainsi 750 000 comptes utilisateurs — nous donne une idée de l'incidence de la communication volontaire sur la protection de la vie privée.

Third, disclosures have involved more than just so-called "basic subscriber information." Indeed, the house committee studying Bill C-13 heard from the RCMP, which noted that "currently specific types of data such as transmission or tracking data may be obtained through voluntary disclosure by a third party.

Fourth, these intermediaries do not notify users about their disclosures, keeping hundreds of thousands of Canadians in the dark. Contrary to some discussion we have heard over the months on C-13, there were no notification requirements within the bill or auditing mechanism.

Fifth, the voluntarily disclosure provision should be viewed in concert with the lack of meaningful changes in Bill S-4, the Digital Privacy Act, which already passed the Senate, that would expand voluntarily warrantless disclosure now to any organization. Given this background, I'd argue that the provision is a mistake and should be removed. It unquestionably increases the likelihood of voluntary disclosures at the very time when Canadians and courts are increasingly concerned with such activity.

You have heard quite a bit about the low threshold for transmission data warrants. This information is commonly referred to as metadata. While some have tried to argue that the metadata is non-sensitive information, that's simply not the case. This information is far more than who phoned whom for how long. It can include highly sensitive information related to computer and computer messaging. As you heard in the prior committee late last year, the Supreme Court of Canada ruled in *R. v. Vu* on the privacy importance of computer-generated metadata, noting:

> In the context of a criminal investigation, however, it can also enable investigators to access intimate details about a user's interests, habits, and identity, drawing on a record that the user created unwittingly . . . .

Security officials have also commented on the importance of metadata. General Michael Hayden, former Director of the NSA and CIA, stated, "We kill people based on metadata." Stewart Baker, former NSA General Counsel, stated that "metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content."

Troisièmement, les renseignements communiqués ne se limitent pas aux renseignements de base des abonnés. En effet, le comité de la Chambre des communes qui a étudié le projet de loi C-13 a accueilli un représentant de la GRC, qui a souligné ce qui suit : « À l'heure actuelle, certains types de données, comme les données de transmission et de suivi, peuvent être obtenus par la divulgation volontaire d'un tiers. »

Quatrièmement, les intermédiaires n'informent pas les utilisateurs de la communication, de sorte que des centaines de milliers de Canadiens ne sont pas informés. Contrairement à certaines des discussions que nous avons entendues au fil des mois au sujet du projet de loi C-13, il n'y a pas d'exigence liée à l'information dans le projet de loi ou dans le mécanisme de vérification.

Cinquièmement, la disposition sur la communication volontaire devrait aussi être examinée parallèlement au manque de modifications importantes dans le projet de loi S-4, la Loi sur la protection des renseignements personnels numériques, qui a déjà été adoptée par le Sénat, ce qui aurait pour effet d'appliquer les dispositions sur la communication volontaire sans mandat à tout organisme. Compte tenu de ce contexte, j'aimerais faire valoir que la disposition est une erreur et qu'elle devrait être retirée. Elle accroît de façon incontestable la probabilité de communication volontaire au moment où les Canadiens et les tribunaux sont de plus en plus préoccupés par de telles activités.

Vous avez beaucoup entendu parler du faible seuil concernant les mandats relatifs aux données de transmission, informations que l'on appelle communément des métadonnées. Certains ont essayé de faire valoir que les métadonnées ne sont pas des renseignements de nature délicate, mais ce n'est tout simplement pas le cas. Cette information dépasse de loin la question de savoir qui a téléphoné à qui et combien de temps a duré la conversation. Cela peut comprendre des informations très délicates liées aux systèmes informatiques et à la messagerie par ordinateur. Comme vous l'avez entendu lors d'une séance antérieure du comité à la fin de l'an dernier, la Cour suprême du Canada, dans l'arrêt *R. c. Vu*, a statué sur l'importance des renseignements personnels associés aux métadonnées générées par ordinateur. Elle a noté ce qui suit :

> Dans le contexte d'une enquête criminelle, cependant, elles peuvent également donner aux enquêteurs accès à des détails intimes sur les intérêts, les habitudes et les identités d'un utilisateur en fonction d'un registre créé involontairement par l'utilisateur...

Des représentants du milieu de la sécurité ont également commenté l'importance des métadonnées. Le général Michael Hayden, ancien directeur de la NSA et de la CIA, a dit : « Nous tuons des gens à cause des métadonnées. » Stewart Baker, ancien avocat général à la NSA, a déclaré ce qui suit : « Les métadonnées disent absolument tout sur la vie d'une personne. Quand vous avez suffisamment de métadonnées, vous n'avez pas vraiment besoin de contenu. »

There are numerous studies that confirm Hayden's and Baker's comments. Some of those studies point to calls to religious organizations that will allow for inferences of a person's religion. Calls to medical organizations allow for inferences on medical conditions. In fact, in a U.S. court brief signed by some of the world's leading computer experts, they noted:

> Telephony metadata reveals private and sensitive information about people. It can reveal political affiliation, religious practices, and people's most intimate associations. It reveals who calls a suicide prevention hotline and who calls their elected official; who calls the local Tea Party office and who calls Planned Parenthood. The aggregation of telephony metadata about a single person over time, about groups of people, or with other datasets only intensifies the sensitivity of the information

Further, the Privacy Commissioner of Canada has released a study on the privacy implications of IP addresses, noting how they can be used to develop a highly personal look at an individual. In fact, even the Justice Minister's report that Senator Batters referred to earlier and served seemingly as the basis for some Bill C-13 recommendations, recommends the creation of new investigative tools but also says that "the level of safeguards increases with the level of privacy interest involved."

Given the level of privacy interest with metadata, the approach in Bill C-13 for transmission data warrants should be amended.

Finally, the lack of transparency, disclosure and reporting requirements associated with warrantless disclosure should be addressed. The stunning revelations earlier this year about requests and disclosure of personal information, the majority of which were without court oversight or warrant, points to an enormously troubling weakness in Canada's privacy laws that *Spencer* only begins to address.

Most Canadians have no awareness of these disclosures and have been shocked to learn how frequently they are used and that bills before Parliament propose to expand their scope. In my view, this makes victims of us all — disclosure of our personal information often without our awareness or explicit consent.

De nombreuses études ont confirmé les commentaires de MM. Hayden et Baker. Certaines études font état d'appels à des organismes religieux qui permettent de tirer des inférences concernant la religion d'une personne et d'appels à des organismes médicaux qui permettent de tirer des inférences touchant l'état de santé de cette personne. De fait, dans un mémoire à un tribunal américain, signé par quelques-uns des plus grands experts mondiaux de l'informatique, on relatait ce qui suit :

> Les métadonnées téléphoniques révèlent des informations à caractère privé et délicat au sujet des gens. Elles peuvent révéler leur affiliation politique, leurs pratiques religieuses et leurs fréquentations les plus personnelles. Elles permettent de savoir qui a téléphoné à une ligne d'aide de prévention du suicide et qui a téléphoné à son député; qui téléphone au bureau local du Tea Party et qui téléphone au service de planification des naissances. Le regroupement des métadonnées téléphoniques — touchant une seule personne sur une période donnée, des groupes de personnes, ou d'autres ensembles de données — augmente davantage le caractère délicat de l'information.

De plus, la commissaire à la protection de la vie privée du Canada a publié une étude sur les répercussions sur les renseignements personnels des adresses IP, où elle dit qu'elles peuvent servir à observer les gens de façon très personnelle. En fait, on voit même dans un rapport du ministre de la Justice, dont la sénatrice Batters a parlé plus tôt et qui semble avoir servi de fondement pour certaines recommandations du projet de loi C-13, une recommandation visant la création de nouveaux outils d'enquête, mais on y indique aussi « que le degré de protection augmente avec l'étendue du droit à la vie privée en jeu. »

Étant donné l'étendue du droit à la vie privée lié aux métadonnées, l'approche proposée dans le projet de loi C-13 en ce qui concerne les mandats visant les données de transmission devrait être modifiée.

Enfin, l'absence de transparence, de divulgation et d'exigence redditionnelle touchant la communication sans mandat devrait être corrigée. Les révélations fracassantes que nous avons entendues plus tôt cette année au sujet des demandes et de la divulgation de renseignements personnels — dans la plupart des cas, sans surveillance des tribunaux ni mandat — montrent du doigt une faiblesse extraordinairement troublante des lois canadiennes en matière de protection des renseignements personnels; la décision *Spencer* n'est qu'un premier pas pour régler ce problème.

La plupart des Canadiens n'étaient pas au courant de ces divulgations et ils ont été choqués d'apprendre à quelle fréquence elles étaient utilisées. Les projets de loi présentés au Parlement visent l'élargissement de leur portée. À mon avis, cela fait de nous tous des victimes, car des renseignements personnels nous concernant pourraient être divulgués souvent sans que nous en ayons connaissance ou sans notre consentement explicite.

I will stop there and welcome your questions.

Senator Baker: These were excellent presentations. It's an honour to have both of you here.

I'd like to direct my first question to Mr. Geist to ask his opinion on the standard way today that police obtain information from Internet service providers. They send a letter to them and say that they are conducting an investigation. Pursuant to section 7(3)(*i*) of PIPEDA, they're requesting information concerning the particular user. What do you think of that provision, Mr. Geist?

Mr. Geist: There have been ongoing concerns about the ability for warrantless disclosure within PIPEDA. In fact, those concerns have been expressed by the Privacy Commissioner of Canada, who was appointed by the current government. When appearing on this bill before the House of Commons committee, the commissioner expressed concern about the lumping together of cyberbullying provisions, which many people think are appropriate and don't have concern with, with lawful access provisions that raise real privacy concerns.

I would have thought that the ability to address some of the issues under PIPEDA might have been addressed under Bill S-4, the Digital Privacy Act. Yet, this did not happen, to the dismay of many, including the Office of the Privacy Commissioner who, when appearing before the Senate committee on this, raised concerns about the potential expansion of voluntary disclosure in this instance to third-party organizations extending beyond law enforcement.

Senator Baker: We've had this law since 2001 on voluntary disclosure. Internet service providers have developed a protocol and they have someone in a department to deal specifically with the police. When you look at disclosure in criminal cases, you see this procedure followed all the time without a warrant. Don't you think it's time it was changed?

Mr. Geist: Certainly, the Supreme Court of Canada thought that. At the end of day, *Spencer* is likely to result in some change in terms of practice. From a law enforcement perspective when obtaining this information, if it ultimately can't be used and if it ultimately proceeds to a court case, it is not particularly helpful but ultimately harmful. Some ISPs have made it clear that they intend to change some of their practices, but not all. In fact, it's worth noting that the lack of transparency and disclosure that I referenced in my opening remarks applies not only to law enforcement but also to our telecom providers, who in many instances have not been forthcoming in terms of their practices. Some of the largest providers, notably Bell, still have not publicly advised their millions of subscribers about how they intend to react to the *Spencer* decision.

Je vais arrêter ici; je suis prêt à répondre à vos questions.

Le sénateur Baker : Il s'agissait d'excellents exposés. C'est un honneur de vous accueillir tous les deux ici.

J'aimerais poser ma première question à M. Geist pour avoir son avis sur les procédures habituelles qu'utilisent actuellement les services de police pour obtenir des informations des fournisseurs de services Internet. Ils leur envoient une lettre disant qu'ils mènent une enquête. Conformément à l'alinéa 7(3)*i*) de la LPRPDE, ils demandent des informations concernant un utilisateur donné. Que pensez-vous de cette disposition, monsieur Geist?

M. Geist : La possibilité d'avoir recours à la communication sans mandat en vertu de la LPRPDE est une préoccupation constante. En fait, ces préoccupations ont été exprimées par le commissaire à la protection de la vie privée, qui a été nommé par le gouvernement actuel. Lorsqu'il a comparu devant le comité de la Chambre des communes pour parler de ce projet de loi, le commissaire s'est dit préoccupé par le regroupement des dispositions sur la cyberintimidation — que beaucoup de gens considèrent comme adéquates et non préoccupantes — et des dispositions relatives à l'accès légal, lesquelles soulèvent de réelles préoccupations en matière de protection de la vie privée.

J'aurais pensé que certains problèmes liés à la LPRPDE auraient pu être réglés dans le projet de loi S-4, la Loi sur la protection des renseignements numériques personnels. Or, cela ne s'est pas produit, au grand désarroi de plusieurs, dont le commissaire à la protection de la vie privée. Lors de sa comparution devant le comité sénatorial pour discuter de cette question, le commissaire a soulevé des préoccupations concernant l'élargissement possible des dispositions sur la communication volontaire, soit, dans ce cas, à des organismes tiers autres que les organismes d'application de la loi.

Le sénateur Baker : Cette loi sur la communication volontaire existe depuis 2001. Les fournisseurs de services Internet ont mis en place des procédures et ont nommé un responsable dans une division quelconque pour traiter avec les services de police. Lorsqu'on se penche sur la communication dans les affaires pénales, on constate que l'on a toujours recours à cette procédure sans mandat. Ne croyez-vous pas qu'il est temps de la modifier?

M. Geist : C'est certainement l'avis de la Cour suprême du Canada. En fin de compte, la décision *Spencer* entraînera probablement une modification des pratiques. Du point de vue des organismes d'application de la loi, lorsqu'on obtient ces informations, mais qu'on ne peut les utiliser et que la cause se rend devant les tribunaux, ce n'est pas particulièrement utile et c'est nuisible, en fin de compte. Certains fournisseurs de services Internet ont clairement indiqué qu'ils ont l'intention de modifier certaines de leurs pratiques, mais ce n'est pas le cas de tous. En fait, il convient de souligner que le manque de transparence et de divulgation dont j'ai parlé dans mon exposé ne s'applique pas seulement aux organismes d'application de la loi, mais aussi aux fournisseurs de services de télécommunications qui, dans bien des cas, ne se sont pas montrés coopératifs au sujet de leurs pratiques.

Certains des plus importants fournisseurs, dont Bell, n'ont toujours pas informé publiquement leurs millions d'abonnés des mesures qu'ils ont l'intention de prendre dans la foulée de la décision *Spencer*.

Senator Baker: There are laws in effect that you think should be changed. Your criticism of this legislation is that you could go to those provisions and stay with the production orders in section 487.012, which is based on a suspicion today in the present Criminal Code. We can talk about reasonable suspicion and so on, but there is it is. It is in the Criminal Code.

Le sénateur Baker : Vous pensez que certaines lois qui sont en vigueur devraient être modifiées. Dans vos critiques à l'égard de cette mesure législative, vous dites qu'en ce qui concerne ces dispositions, vous conserveriez les ordonnances de communication prévues à l'article 487.012 de l'actuel Code criminel, qui sont fondées sur le soupçon. Nous pouvons parler de soupçons raisonnables, notamment, mais cela existe déjà. C'est dans le Code criminel.

Both of you are saying that times have changed in that under the normal investigative procedures regarding the interception of private communications, which normally involves a 487 warrant, a 492.2, which is a dialed-number recorder warrant, and a 186 warrant to intercept private communications, should change because the second one is on a suspicion. Both of you are saying that that second one as it relates to the Internet should be on "reasonable grounds to believe," which is the same standard that is used for the interception of private communication. Is that correct?

Vous affirmez tous les deux que les temps ont changé et qu'on devrait modifier les procédures habituelles d'enquête concernant l'interception des communications privées, qui exigent habituellement un mandat aux termes de l'article 487, un mandat aux termes de l'article 492.2, c'est-à-dire un mandat lié aux enregistreurs de numéros composés, et un mandat aux termes de l'article 186 lié à l'interception des communications privées, car l'obtention du deuxième est fondée sur un soupçon. Vous dites tous les deux que le deuxième mandat, en ce qui concerne Internet, devrait être fondé sur « des motifs raisonnables de croire », c'est-à-dire la norme utilisée pour l'interception des communications privées. Est-ce exact?

Ms. Slane: The initial impetus for that was a different technology. Different information could be obtained from a dialed-number recorder 20 years ago when that standard seemed appropriate than there is now. That's clear. If you were updating things, you could keep the dialed-number recorder if "dial" means something different than transmission data. If it doesn't, if a dialed-number recorder is now a transmission-data recorder, which is something similar in terms of how we now communicate, then yes, we do need to update that older provision as well to match that if people aren't using something similar to what that technology was back in the day. That makes some sense to me.

Mme Slane : Lors de leur mise en œuvre, ces mesures visaient une technologie différente. Il y a 20 ans, on pouvait obtenir différents renseignements à l'aide d'un enregistreur de numéros composés, et cette norme semblait clairement plus appropriée que maintenant. Si vous faisiez une mise à jour, vous pourriez conserver l'enregistreur de numéros composés si « composés » représente autre chose que la transmission de données. Toutefois, si un enregistreur de numéros composés est maintenant un enregistreur de transmission de données, un dispositif similaire en ce qui concerne notre façon de communiquer, dans ce cas, nous devons également mettre à jour cette ancienne disposition pour qu'elle vise la nouvelle technologie utilisée, si elle est différente. Cela me semble logique.

I would like to add that it seems to me there is some restraint within PIPEDA that has not been fully explored either, which is that people who are subject to PIPEDA, the private companies, including Internet service providers, have to act reasonably within the circumstances, even with regard to section 7. So it would seem that they do have some obligations, even within that legislation, not to just provide information upon request. It has to be something that actually fits the circumstances.

J'aimerais ajouter qu'il me semble qu'on a négligé d'explorer une certaine retenue présente dans la LPRPDE, et que les personnes assujetties à la LPRPDE, les entreprises privées — y compris les fournisseurs de service Internet —, doivent agir de façon raisonnable dans les circonstances, même en ce qui concerne l'article 7. Il semble donc que ces personnes soient tenues, même dans le cadre de cette loi, de ne pas seulement fournir des renseignements sur demande. Il faut que cela corresponde aux circonstances.

Senator Plett: Mr. Geist, you have testified that a balance has to be struck between upholding the right of privacy and fighting online harms. I think we all agree that a balance needs to be struck. I think the discussion is: What is the right balance?

Le sénateur Plett : Monsieur Geist, selon votre témoignage, il faut atteindre un équilibre entre le maintien du droit à la vie privée et la lutte contre les infractions commises en ligne. Je crois que nous convenons tous qu'il faut atteindre cet équilibre. Toutefois, je crois qu'il faut déterminer le bon équilibre.

Two weeks ago, we hear from Mr. Gilhooly, who was a victim of sexual assault as a child and who is now a lawyer. He testified before us, saying:

> . . . privacy rights are going to have to be compromised to ensure that we live in a safe society where our police have adequate tools.
>
> That doesn't, in my view, mean that we're living in a police state, that we have to live in a police state. That means that we have to take, as a collective, a view in terms of what do we need and what do we require to ensure that commonsensical results take place.

Later, in response to a question that my colleague Senator Frum had about privacy, he discussed privacy in the modern connected word, concluding:

> In terms of this legislation, it won't impact the average Canadian one iota.

I would just like your comment on his comment, if you would.

Mr. Geist: Off the cuff, I'd raise three things. First, I think you're right that everybody does agree that we are talking ultimately about a balance here and where to strike that balance. That said, if the witness that you heard from last week suggests somehow that we dispense with privacy because this is what law enforcement needs, I would submit that the Charter doesn't say that. The ultimate law of the land, at this stage, doesn't say that we dispense with privacy. Privacy remains something that's absolutely crucial.

But within this context, it seems to me that we are talking about how to deal with that balance. What you heard from me, and what I think the committee has heard many times, is that when we talk about the need for appropriate oversight, that doesn't hamstring law enforcement. That doesn't say that we get rid of privacy or that we don't provide the tools. That says that we have real concerns about expanding voluntary disclosure, as this bill seeks to do and as Bill S-4 sought to do, so that you are expanding the likelihood of disclosure without any oversight. I'm not saying not to disclose; in the appropriate circumstances, without question. I'm saying that you don't do it without oversight, and if you expand the likelihood of voluntarily disclosure, you are removing the likelihood of that oversight.

Second, if we are talking about this issue of threshold, as we just did a moment ago with metadata, the core point to recognize is that the kind of information that can be gleaned from metadata very often is now what we would have thought of as content a decade or so ago. We recognized very easily that content was somehow deeply sensitive. It says a whole lot about stuff, and yet somehow we thought back then, partially because the technology was not where it is today, that metadata did not have that same

Il y a deux semaines, nous avons entendu le témoignage de M. Gilhooly, qui a été victime d'agression sexuelle lorsqu'il était enfant; il est maintenant avocat. Voici ce qu'il nous a dit :

> [...] le droit à la vie privée devra faire l'objet d'un compromis si nous voulons vivre dans une société sûre où les policiers disposent d'outils adéquats.
>
> À mon avis, cela ne veut pas dire que nous vivons dans un État policier ou que nous devons vivre dans un État policier. Cela veut dire que nous allons devoir, collectivement, nous faire une idée de ce dont nous avons besoin pour obtenir des résultats qui ont du bon sens.

Plus tard, en réponse à une question posée par ma collègue, la sénatrice Frum, sur la protection de la vie privée, il a parlé de la vie privée à l'ère d'Internet en terminant avec ceci :

> En conséquence, ce projet de loi ne changera pas d'un iota la vie d'un Canadien moyen.

J'aimerais seulement avoir votre avis sur son commentaire.

M. Geist : J'aimerais d'emblée soulever trois points. Tout d'abord, je crois que vous avez raison : tout le monde convient qu'au bout du compte, nous parlons d'un équilibre et de l'atteinte de cet équilibre. Cela dit, si le témoin que vous avez entendu la semaine dernière a suggéré, en quelque sorte, que nous cessions de protéger la vie privée pour faciliter le travail des organismes d'application de la loi, je ferais valoir que ce n'est pas ce que prévoit la Charte. En ce moment, nos lois ne suggèrent pas d'éliminer la protection de la vie privée. C'est un élément qui demeure essentiel.

Toutefois, dans ce contexte, il me semble que nous cherchons la bonne façon d'atteindre cet équilibre. Ce que j'ai dit, et je crois que les membres du comité l'ont entendu à de nombreuses reprises, c'est que la nécessité d'exercer une surveillance appropriée n'entrave pas l'application de la loi. Cela ne signifie pas que nous devrions éliminer la protection de la vie privée ou cesser de fournir les outils nécessaires. Cela signifie que nous sommes réellement préoccupés par l'accroissement de la divulgation volontaire proposée par ce projet de loi et le projet de loi S-4, car on accroît ainsi la probabilité de divulgation sans surveillance. Je ne dis pas qu'il faut empêcher la divulgation; il ne fait aucun doute qu'elle est nécessaire dans les circonstances appropriées. Je dis seulement qu'il ne faut pas le faire sans surveillance, et que si nous accroissons la probabilité de divulgation volontaire, nous éliminons la probabilité qu'on exerce cette surveillance.

Deuxièmement, si vous parlez de la question du seuil, comme nous l'avons fait il y a quelques instants avec les métadonnées, il est important de reconnaître que le type de renseignement qui peut être obtenu à partir des métadonnées est très souvent, maintenant, ce que nous aurions considéré comme étant du contenu il y a environ 10 ans. Nous avons reconnu très facilement que le contenu était, en quelque sorte, de nature extrêmement délicate. Il fournit beaucoup de renseignements sur certains

kind of privacy import. It does today. If the former witness suggests that we should dispense with oversight and the right thresholds, I think he's wrong.

Finally, I would point out that if he thinks that this does not affect the average Canadian, he is absolutely wrong. I also talk to high school kids and was in one of my kids' high schools talking with some of their cohort. When we talked about Bill C-13 and Bill S-4, it involved not only a discussion of the cyberbullying provisions but also the prospect of what would happen if who they were communicating with, with other pieces of information, might also be accessed at a very low threshold. They were deeply concerned with the impact of that kind of thing.

One need only look at the headlines that we've seen here and elsewhere over the last number of weeks to know what metadata can mean. Think of the communications that might have taken place between a couple of members of Parliament now accused of harassment and other MPs. All someone would want is not to know the content of these emails but simply to know who they were communicating with and when they were communicating because that information would have enormous impact.

Think of those who have come forward in the Jian Ghomeshi case. It's not a matter of what was said. It's merely a matter of metadata involved that can be enormously revealing and have a huge impact. What I'm saying, and what many others have said, is that if you are going to have that information disclosed it's essential that it be at an appropriate threshold.

Senator Joyal: Taking into consideration the conclusion of the Supreme Court's *Spencer* decision in June, would you think that if that bill passes the way it is, the next step is that someone who is the object of an accusation in relation to possession of images relating to kids could fight that accusation on the basis that the proof would have been illegally obtained by the police force and that the case could be dismissed?

Mr. Geist: I'm not a criminal defence lawyer, but I suppose it will depend upon how law enforcement got that information and how it ultimately gets used in the case.

Senator Joyal: On the basis of the principles in *Spencer*.

Mr. Geist: Yes, on the basis of *Spencer*, if we are talking about the transmission-data warrant, if they go out and get the warrant and that's the threshold, I think there's no doubt that that puts it at potential risk. You only need to read the decision, along with *Vu* and a series of other cases that have come from the court. Plus, we'll get the *Fearon* case fairly soon as well. The court has now created four or five privacy cases in which they really have sought to update privacy law for the current technological environment. They, frankly, better than this legislation, have recognized the

éléments et pourtant, à l'époque, en partie parce que la technologie n'était pas aussi avancée qu'aujourd'hui, nous pensions que les métadonnées n'offraient pas autant de renseignements personnels. Elles le font aujourd'hui. Si votre ancien témoin laisse entendre que nous devrions éliminer la surveillance et les seuils appropriés, je crois qu'il a tort.

Enfin, j'aimerais souligner que s'il est d'avis que cela ne touche pas le Canadien moyen, il a absolument tort. J'ai parlé à des élèves du secondaire et j'ai parlé à certains élèves de l'école secondaire que fréquente l'un mes enfants. Lorsque nous avons parlé des projets de loi C-13 et S-4, la discussion n'a pas seulement porté sur les dispositions sur la cyberintimidation, mais également sur ce qui arriverait si le seuil pour avoir accès à la personne avec laquelle ils communiquent, avec d'autres éléments de renseignement, était très bas. Ils étaient extrêmement préoccupés par ce genre de répercussions.

On n'a qu'à lire les manchettes des dernières semaines d'ici et ailleurs pour se faire une idée de la signification des métadonnées. Pensez aux communications qui peuvent avoir eu lieu entre les deux députés du Parlement qui sont maintenant accusés de harcèlement et d'autres députés. Il n'est pas nécessaire de connaître le contenu des courriels, mais simplement de connaître leurs interlocuteurs et le moment des communications, car ces renseignements entraîneront d'énormes répercussions.

Pensez aux personnes qui ont témoigné dans l'affaire concernant Jian Ghomeshi. L'important, ce n'est pas ce qui a été dit, mais les métadonnées qui pourraient révéler beaucoup de choses et entraîner d'énormes conséquences. Ce que je fais valoir, comme l'ont fait de nombreuses autres personnes, c'est que si on divulgue ces renseignements, il est essentiel d'établir un seuil approprié.

Le sénateur Joyal : À votre avis, en tenant compte des conclusions qu'a formulées la Cour suprême en juin dans la décision *Spencer*, si le projet de loi est adopté dans sa forme actuelle, une personne accusée de possession d'images représentant des enfants pourrait-elle dorénavant contester cette accusation en alléguant que la police a obtenu les preuves illégalement et que l'affaire doit être rejetée?

M. Geist : Je ne suis pas un avocat de la défense en droit criminel, mais je présume que cela dépendra de la façon dont les organismes d'application de la loi ont obtenu ces renseignements et de la façon dont ils sont utilisés dans l'affaire.

Le sénateur Joyal : Sur le fondement des principes déterminés dans la décision *Spencer*.

M. Geist : Oui, si l'on se fonde sur la décision *Spencer*, je crois qu'un mandat lié à la transmission de données obtenu selon ce seuil présente, sans aucun doute, un risque potentiel. Vous n'avez qu'à lire cette décision, ainsi que la décision *Vu* et une série d'autres décisions rendues par les tribunaux. De plus, nous pourrons bientôt lire la décision *Fearon*. Le tribunal a maintenant créé quatre ou cinq décisions liées à la protection de la vie privée et dans lesquelles il a vraiment tenté d'actualiser la Loi sur la vie privée pour qu'elle corresponde à l'environnement technologique

privacy implications. If law enforcement seeks to rely on information obtained via a warrant with that lower threshold, I don't think there is any doubt that a defence attorney will seek to challenge the validity of that warrant as having a threshold that's far too low.

Senator Joyal: Of course, if that proof is brought to the court, the defence lawyer will fight the fact that the proof has been illegally obtained, that is, contrary to the protection that the Charter affords to someone to be unreasonably searched, to get some elements of facts that are not admissible as proof.

Mr. Geist: Sure, and that's what I thought you heard from the criminal lawyers earlier. I would like to even extend the damage this causes for those who are hoping to ensure that law enforcement has the appropriate tools. I keep hearing that law enforcement needs the tools, and it seems like everybody is in agreement on that. Think of the expansion of voluntary disclosure creating this immunity. I don't think you will see many ISPs disclosing voluntarily anymore in a post-*Spencer* environment. You have a provision that purports to help to expand some of that voluntarily disclosure to help law enforcement. You now have a Supreme Court of Canada decision that makes it clear that most ISPs are not going to cooperate at all, and in the event that they do, you have a clear opportunity for a challenge anyway based on what we had in *Spencer*.

If you are generally concerned about providing law enforcement with the tools they need to deal with this issue, why on earth would anybody, in a post-*Spencer* environment, move forward with an attempt to try to expand voluntary exposure? That's the part that I find so puzzling from the Justice Minister, who, in the aftermath of *Spencer*, has tried to argue that nothing changed. The thing that changed is that if you are serious about trying to give law enforcement the tools they need, you can't use the voluntary approach. The Supreme Court just told you that.

Senator Joyal: The other element that concerns me is that when there is a challenge on a provision of a Charter, there are always three questions that the court will walk through. The first is: What is the purpose of the legislation? Is it a sound purpose? Second, does the measure proposed in the legislation under discussion serve the objective that the purpose is supposed to get? Third, is it the least intrusive? In my opinion, the least intrusive question will fail because at least presently, when you get a search warrant or an authorization to tap someone's line, you have to inform the person after that you have done it in order for there to be a balance, but not with this anymore. Now you can get much more information than the wiretap and you don't even have the obligation to inform the person that you got all the information

actuel. Honnêtement, ces décisions reconnaissent mieux les conséquences sur la vie privée que le projet de loi. Si les organismes d'application de la loi souhaitent compter sur des renseignements obtenus par l'entremise d'un mandat assujetti à ce seuil moins élevé, je crois qu'il ne fait aucun doute qu'un avocat de la défense cherchera à contester la validité de ce mandat en faisant valoir que le seuil est beaucoup trop bas.

Le sénateur Joyal : Manifestement, si cette preuve est présentée devant le tribunal, l'avocat de la défense contestera le fait que la preuve a été obtenue illégalement, c'est-à-dire de façon contraire à la protection contre une fouille déraisonnable conférée par la Charte et qu'il s'agit d'éléments qui ne sont pas admissibles comme preuve.

M. Geist : Évidemment, et je crois que c'est ce que vous avez entendu de la part des avocats au criminel plus tôt. J'aimerais même accroître le préjudice causé par cette mesure pour ceux qui souhaitent veiller à ce que les organismes d'application de la loi possèdent les outils appropriés. J'entends toujours dire que les organismes d'application de la loi ont besoin des outils nécessaires, et il semble que tout le monde s'entend là-dessus. Pensez à l'accroissement de la divulgation volontaire qui crée cette immunité. Je ne crois pas que de nombreux fournisseurs de services Internet divulgueront volontairement des renseignements après la décision *Spencer*. On a une disposition qui est censée accroître certaines de ces divulgations volontaires pour aider les organismes d'application de la loi. On a maintenant une décision de la Cour suprême du Canada qui énonce clairement que la plupart des fournisseurs de services Internet ne coopéreront pas du tout, et que même s'ils le faisaient, il est possible de contester leur témoignage sur le fondement de la décision *Spencer*.

Si vous avez des préoccupations générales sur le fait de fournir aux organismes d'application de la loi les outils dont ils ont besoin pour s'attaquer à ce problème, pourquoi tenterait-on, après la décision *Spencer,* d'accroître la divulgation volontaire? C'est ce que je trouve vraiment intrigant au sujet du ministre de la Justice qui, après la décision *Spencer,* a tenté de faire valoir que rien n'avait changé. Ce qui a changé, c'est que si vous tentez sérieusement de fournir aux organismes d'application de la loi les outils dont ils ont besoin, vous ne pouvez pas utiliser l'approche volontaire. La Cour suprême vient de vous le confirmer.

Le sénateur Joyal : L'autre élément qui me préoccupe, c'est que lorsqu'il y a une contestation fondée sur une disposition de la Charte, le tribunal examine toujours trois questions. Tout d'abord, quelle est la raison d'être de la loi? Est-elle valable? Deuxièmement, les mesures proposées dans la loi concernée servent-elles les objectifs visés par la raison d'être de la loi? Troisièmement, est-ce la mesure la moins intrusive? À mon avis, la question de la mesure la moins intrusive échouera, car actuellement, lorsqu'on obtient un mandat de perquisition ou une autorisation de mettre quelqu'un sur écoute, il faut informer la personne visée après l'avoir fait, afin d'atteindre un équilibre, mais on n'a plus besoin de le faire avec cette mesure. Maintenant, on peut obtenir beaucoup plus de renseignements qu'avec l'écoute

about the privacy of that person. It seems to be one of the key elements that will bring those measures to fail in the court. Can you comment on that?

Ms. Slane: One of things that has been puzzling, because a lot of strategy has been going on for 10 years now, is that the *Spencer* case highlighted that they were testing voluntary disclosure capabilities. They had cases where they could have gotten a warrant. In all of those child pornography cases, they had the smoking gun. They had the image and could have easily established the highest standards of "reasonable grounds to believe" that the crime had been committed. It was all there, but they did it in order to see if this would fly with the Charter and it failed.

There were lots of disclosures that ISPs gave in the course of that time which were not in the service of child pornography investigations but all other types of requests. Those are not coming to the courts and being challenged because they are not relying on those to get further warrants where someone presents the evidence in court.

One of the problems, without having any oversight, is there is a whole lot of collection that goes on and does not come to anyone's attention because they are smarter than that. They are not going to put it in the court's face if it is potentially questionable. There is other damage that could be done by this type of bill that will be very difficult to bring to under Charter scrutiny.

Senator Batters: Mr. Geist, you were speaking about Carol Todd, Amanda Todd's mom. She met with the Minister of Justice after her House of Commons appearance and did an interview on CBC radio. Did you hear that interview or see a transcript, because she clarified her views on the bill.

Mr. Geist: Not only did I hear that, but I got an email from her days after this bill passed in the House of Commons, expressing dismay that the bill had not been changed and that victims like her, who had expressed concern about privacy, had not been heard.

Senator McIntyre: Thank you both for your presentations. I will move your attention away from some of the issues that have been raised.

I draw your attention to section 162.1(2) of the bill. That clause deals with a definition of "intimate image." I will not read out that section, however, I understand it contains a three-part definition of intimate images. First, it appears to me that there is

électronique et on n'est même pas tenu d'informer la personne de tous les renseignements qu'on a recueillis à son sujet. Il semble que c'est l'un des éléments principaux qui feront échouer ces mesures devant le tribunal. Pourriez-vous commenter cela?

Mme Slane : L'une des choses déroutantes, car un grand nombre de stratégies ont été mises en œuvre durant les deux dernières années, c'est que la décision *Spencer* a souligné le fait qu'on testait les capacités de divulgation volontaire. Dans certains cas, on pourrait avoir obtenu un mandat. Dans toutes ces affaires de pornographie infantile, on avait des preuves flagrantes. On avait les images et on aurait pu facilement satisfaire aux normes les plus élevées de « motifs raisonnables de croire » que l'infraction criminelle avait été commise. Tous les éléments nécessaires étaient présents, mais on a agi de cette façon pour vérifier si cela répondait aux critères de la Charte, et cela a échoué.

De nombreux éléments divulgués par les fournisseurs de services Internet pendant ce temps n'ont pas servi aux enquêtes sur la pornographie infantile, mais à tous les autres types de demandes. Ils ne sont pas présentés et contestés devant les tribunaux, car on ne compte pas sur eux pour obtenir d'autres mandats lorsqu'une personne présente des preuves devant le tribunal.

L'un des problèmes, lorsqu'on n'exerce aucune surveillance, c'est qu'on recueille une grande quantité de données et de renseignements et que personne ne s'en aperçoit, car on est prudent. On ne va pas présenter ces renseignements devant le tribunal s'ils peuvent potentiellement faire l'objet d'une contestation. Ce type de projet de loi pourrait entraîner d'autres préjudices qui seront très difficiles à contester en vertu de la Charte.

La sénatrice Batters : Monsieur Geist, vous avez parlé de Carole Todd, la maman d'Amanda Todd. Elle a rencontré le ministre de la Justice après avoir comparu devant la Chambre des communes, et elle a donné une entrevue à CBC Radio. Avez-vous entendu cette entrevue ou avez-vous lu une transcription, car elle a clarifié son opinion sur le projet de loi.

M. Geist : Non seulement je l'ai entendue, mais elle m'a envoyé un courriel quelques jours après l'adoption du projet de loi à la Chambre des communes pour exprimer son désarroi sur le fait que le projet de loi n'avait pas été modifié et que les victimes comme elle, qui avaient exprimé des préoccupations liées à la protection de la vie privée, n'avaient pas été entendues.

Le sénateur McIntyre : Je vous remercie de vos exposés. Je dois détourner votre attention des questions qui ont été soulevées.

J'aimerais plutôt attirer votre attention sur le paragraphe 162.1(2) du projet de loi. Ce paragraphe traite de la définition d'« image intime ». Je ne lirai pas le paragraphe, mais d'après ce que je comprends, il contient une définition en trois

clarity in the determination and specific warning of what classifies as an intimate image. As you know, the definition is similar to the one found in child pornography offences.

Second, it's clear that there is an expectation of privacy at the time the image was taken. In other words, it was done in circumstances that gave rise to the reasonable expectation of privacy, and finally the person had retained an expectation of privacy.

I'm satisfied with that definition and I wonder if you are satisfied with it. The reason I'm asking that question is because most if not all the sections found in this bill rotate around the definition of intimate image.

Ms. Slane: I'm basically satisfied with that. If anything, I've had some reason to be questioning the last bit in that I have had concerns on what it takes to lose your reasonable expectation of privacy in an image. I don't think this bill wants it, but I wanted it to be clear that because an image got out, you then no longer have that expectation to be able to control it. There is some point down the line where the image is now out there in the world and therefore you've lost your reasonable expectation of privacy in that intimate image.

I would not want that to happen necessarily, although important points have been made about where the lines are going to be drawn, especially when the images go viral and circulate so much that you cannot charge your way out of those situations. You can't charge 1,000 people for having shared an image. Nevertheless, I would not want to see us establish some sort of standard by which a person, because their image has been circulating, has lost their expectation of privacy.

Mr. Geist: My area is more on the privacy side. I don't feel I'm in a position to respond specifically to this. In some ways it highlights why, as the Privacy Commissioner of Canada, Mr. Therrien, noted, this bill should have been divided into two. We would have had the opportunity to more carefully study these issues on the cyberbullying side and ensure we had effective tools to deal with it, and perhaps separately deal with these lawful access provisions.

Senator Frum: I'm a digital immigrant. I ask this question sincerely on the issue of metadata.

If law enforcement gets a transmission data warrant, will they have more access on a metadata level to my information, or any Canadian's information, than Facebook or Google already has?

parties de l'expression « image intime ». Tout d'abord, il me semble qu'on a déterminé clairement ce qui constitue une image intime et qu'on a émis des avertissements précis. Comme vous le savez, la définition est similaire à celle qu'on trouve dans les infractions liées à la pornographie infantile.

Deuxièmement, il y a clairement des attentes liées à la protection de la vie privée lorsque l'image est prise. Autrement dit, elle est prise dans des circonstances pour lesquelles il existe une attente raisonnable de protection en matière de vie privée et enfin, la personne avait toujours des attentes liées à la protection de la vie privée.

Je suis satisfait de cette définition, et j'aimerais savoir si vous l'êtes aussi. Je pose la question, car la plupart, sinon tous les articles contenus dans le projet de loi tournent autour de la définition d'image intime.

Mme Slane : Je suis essentiellement satisfaite. J'ai eu quelques raisons de remettre en question la dernière partie, car je me demandais dans quelles circonstances on perd les attentes raisonnables concernant la protection de la vie privée relativement à une image. Je ne crois pas que ce soit l'intention du projet de loi, mais je voulais établir clairement que lorsqu'une image est diffusée, on perd ces attentes liées au contrôle de celle-ci. Il y a un certain moment où l'image est diffusée et où l'on perd toute attente raisonnable liée à la protection de la vie privée à l'égard de cette image intime.

Je ne voudrais pas nécessairement que cela se produise, même si on a soulevé des points importants en ce qui concerne les limites qui seront fixées, surtout lorsque les images deviennent virales et sont tellement diffusées qu'on ne peut pas porter d'accusations pour échapper à cette situation. En effet, on ne peut pas accuser 1 000 personnes d'avoir partagé une image. Néanmoins, je ne voudrais pas qu'on établisse une norme qui force une personne à renoncer à ses attentes liées à la protection de la vie privée parce que son image a été diffusée.

M. Geist : Je m'occupe davantage de l'élément lié à la protection de la vie privée. Je ne crois pas être en position de répondre à cette question. De certaines façons, cela explique pourquoi M. Therrien, le commissaire à la protection de la vie privée du Canada, a souligné que le projet de loi aurait dû être divisé en deux parties. On aurait eu l'occasion d'étudier plus en détail les enjeux liés à la cyberintimidation et de veiller à ce que nous ayons des outils efficaces pour s'attaquer à ce problème, et peut-être d'examiner ensuite, de façon distincte, les dispositions sur l'accès légal.

La sénatrice Frum : Je suis une immigrante du numérique. J'ai sincèrement posé cette question relativement à l'enjeu des métadonnées.

Si les agents d'application de la loi reçoivent un mandat de perquisition pour obtenir des données de transmission, auront-ils accès à plus de métadonnées me concernant ou concernant tout autre Canadien que Facebook ou Google?

Mr. Geist: Yes, of course. Facebook and Google have only the information that you reveal to them. If you are interacting directly with Facebook, and you have certain cookie information, they can track certain amounts of activity where you've gone to websites that have a Facebook widget embedded. They don't see who you email or sites you visit that don't have a Facebook widget. You can anonymize yourself and simply not use a Facebook widget. Similarly with Google, you can use it without logging in at all and Google does not track anything about who you are specifically.

Senator Frum: That is not how it feels when I get targeted email.

Mr. Geist: They are able to target, on an anonymous basis, a particular IP address. In an email situation, they are simply canvassing the content, on an automatic basis, on what is in the email and coming up with something they think would be relevant.

That is a far cry from the ability to access all of your correspondence, regardless of who it is with and under what circumstance, as a transmission data warrant would. There is not even close to a comparison.

Senator Frum: On the concept of reasonable expectation of privacy, isn't it fair to say that there is much less privacy than most of us Internet users appreciate or recognize as is? So when you're trying to find that level of reasonable expectation, you have to remove the ignorance out of it for people who use Facebook or Google; it is not actually private. Facebook is monitoring every single transmission you make. They hang on to it, own it, monitor it, target you and market to you and sell it. They don't respect your privacy at all. I'm very anti-Facebook.

Ms. Slane: One of the things Michael has been saying is what is different about when law enforcement does it is that they would potentially have the capacity to compile all of those things. It's your transactions with all the social media sites, plus the places where you browse, things you are taking a look at, people you call, things you are inquire about. It's being able to pull all those things together, which is more invasive than what one social media company gets.

In terms of what is reasonable, there is the normative standard. If you are used to having your privacy violated, it does not change. It's still in relationship to what we expect in a democratic society. Just because you are used to being treated terribly by your company doesn't mean that the privacy standards we want to uphold as a democratic society adjust to that.

Senator Frum: If I was using one of those interface mechanisms, in fact I am being completely monitored at all times, whether I'm aware of it or not.

M. Geist : Oui, bien sûr. Facebook et Google ne possèdent que les renseignements qu'on leur révèle. Si vous interagissez directement avec Facebook et que vous avez certains témoins, ils pourront suivre une partie de vos activités si vous avez consulté des sites web qui contiennent un widget Facebook. Ils ne verront pas les sites consultés qui ne comportent pas de widget Facebook ni à qui vous avez envoyé des courriels. Vous pouvez vous rendre anonyme en n'utilisant simplement pas de widget Facebook. C'est la même chose pour Google, vous pouvez l'utiliser sans vous connecter, et Google ne recueillera aucune donnée sur votre identité.

La sénatrice Frum : Ce n'est pas l'impression que j'ai quand je reçois des courriels ciblés.

M. Geist : Ils peuvent cibler, de façon anonyme, une adresse IP en particulier. Pour les courriels, ils vont simplement analyser le contenu, de façon automatisée, pour connaître l'objet des courriels, puis faire des propositions qui leur semblent pertinentes.

C'est très loin de l'accès à toute la correspondance, quelles qu'en soient la provenance et les circonstances, que permet un mandat sur les données de transmission. Cela ne se compare même pas.

La sénatrice Frum : Sur le concept des attentes raisonnables de protection en matière de vie privée, serait-il juste de dire qu'il y a beaucoup moins de confidentialité que la plupart des internautes comme nous ne le croient? Pour satisfaire ces attentes raisonnables, il faut mettre fin à l'ignorance de tous les utilisateurs de Facebook ou de Google : leurs activités ne sont pas vraiment privées. Facebook suit chaque transmission de données. Il s'accroche, se rend propriétaire des données, les suit, procède au ciblage et à la commercialisation des données d'identité et les vend. Il ne respecte pas du tout la vie privée. Je suis farouchement contre Facebook.

Mme Slane : Michael essaie de vous expliquer que la différence, c'est que les agents d'application de la loi auraient le pouvoir de compiler toutes ces données. Je parle des transactions avec les médias sociaux dans leur ensemble, mais aussi de tous les autres sites que la personne visite, de ce qu'elle regarde, des personnes qu'elle appelle, des recherches qu'elle fait. Ils peuvent rassembler toutes ces données, ce qui est beaucoup plus invasif que ce qu'un média social peut faire à lui seul.

Pour déterminer ce qui est raisonnable, il y a une norme. Elle n'est pas différente pour la personne habituée à ce qu'on porte atteinte à sa vie privée. Elle continue de se fonder sur ce à quoi on s'attend dans une société démocratique. Ce n'est pas parce qu'une personne est habituée à être maltraitée par son entreprise que les normes de confidentialité que nous voulons protéger en tant que société démocratique seront aussi médiocres.

La sénatrice Frum : Si j'utilise l'une de ces interfaces, je suis en fait totalement surveillée en tout temps, que j'en sois consciente ou non.

Mr. Geist: No. When you are on the service, with your consent, you signed up and they offered up a privacy policy and a whole species of different mechanisms that you can choose in terms of how much information you share, how that information is used and the like. These are choices that you ultimately make, and of course you can choose not to use it altogether. They are able to collect and use that, which is not the same as tracking all Internet-based activity. The equivalent of saying that Facebook and "this" are the same, is on the one hand saying I'm going to log out of Facebook and on the other hand I'm going to log off communication altogether. That's not the same thing. I can decide that I don't want to use Facebook.

I would submit that it is not practical for almost any Canadian at this point in time to simply say they won't communicate any more using our computer networks as well as our phone networks. Yet that is what is being captured. That's a far cry and much different from what Facebook is able to capture, as people opt into it.

Senator Frum: I don't want Google tracking me, but they do.

Mr. Geist: They only track you if you allow them to track you. You can surf Google and you can the search functionality without any profile, without logging in, and it's done on an anonymous basis.

Senator Frum: You'll have to tell me how to do that later.

[*Translation*]

Senator Dagenais: Mr. Geist, you are aware that most internet service providers have policies on the acceptable use of their service and that the policies contain guidelines for the users of the Internet service. Do you feel that those policies are effective enough to stop cyberbullying? If not, what could be added to those policies to make them more effective?

[*English*]

Mr. Geist: I've looked at some of those network provider policies in a number of different contexts, and quite frankly most providers grant for themselves the right to do just about anything on their networks in terms of what subscribers do on their networks.

I think the short answer is, sure, ISPs have the power. They grant themselves, at least contractually, the power to turn somebody off or to say that they're going to cease to be a customer or to say that it's violating any number of different rules that they've identified with respect to network behaviour. But that's that direct contractual relationship between ISP and the subscriber.

M. Geist : Non. Quand vous adhérez à un service, vous consentez, par votre signature, à la politique de protection de la vie privée qu'il vous offre, et il y a toute une série de mécanismes qui vous permettent de choisir quels renseignements vous voulez partager, comment ils seront utilisés et tout le reste. Ce sont des choix que chacun fait, mais bien sûr, on peut aussi choisir de ne pas les utiliser du tout. Ces services sont ensuite en mesure de recueillir et d'utiliser les données en question, ce qui ne se compare pas à un suivi de toutes les activités sur Internet. Quand vous dites que c'est la même chose pour Facebook, c'est comme si vous disiez qu'en vous déconnectant de Facebook, vous alliez vous couper de toute forme de communication. Ce n'est pas la même chose. Je peux décider de ne pas utiliser Facebook.

Je crois qu'il ne serait pas réaliste pour la plupart des Canadiens en ce moment de décider de ne plus communiquer du tout à l'aide des réseaux informatiques ou cellulaires. C'est pourtant l'idée ici. C'est très différent de ce que Facebook permet de faire, puisque les utilisateurs doivent y donner leur consentement.

La sénatrice Frum : Je ne veux pas que Google suive mes activités, mais il le fait.

M. Geist : Il ne le fait que si vous lui permettez de le faire. Vous pouvez naviguer à l'aide de Google et utiliser la fonction de recherche sans profil, sans vous connecter, dans l'anonymat.

La sénatrice Frum : Vous devrez m'expliquer comment le faire un peu plus tard.

[*Français*]

Le sénateur Dagenais : Monsieur Geist, vous êtes au courant que la plupart des fournisseurs de service Internet ont des politiques relatives à l'utilisation acceptable de leur service et, d'ailleurs, ces politiques contiennent des lignes directrices destinées aux utilisateurs de service Internet. Pensez-vous que ces politiques sont assez efficaces pour éviter la cyberintimidation? Si ce n'est pas le cas, qu'est-ce qu'on pourrait ajouter à ces politiques pour qu'elles soient plus efficaces?

[*Traduction*]

M. Geist : J'ai examiné les politiques de quelques fournisseurs de service dans divers contextes, et bien honnêtement, la plupart s'accordent le droit de faire à peu près n'importe quoi sur leur réseau par rapport aux activités de leurs abonnés.

Je pense qu'en quelques mots, les fournisseurs de services Internet ont effectivement ce pouvoir. Ils s'accordent, à tout le moins par contrat, le pouvoir de débrancher une personne, de refuser un consommateur ou de statuer qu'il contrevient à certaines règles régissant les comportements sur le réseau. Toutefois, tout cela relève de la relation contractuelle directe entre le fournisseur de services et l'abonné.

This issue came up also in *Spencer* with the argument being that somehow people didn't have a reasonable expectation of privacy because ISPs were trying to limit what their expectation might be based on those terms. The court rejected that, noting that importing that contract, essentially signing away or clicking away your reasonable expectation of privacy, to them didn't seem reasonable under those circumstances.

[*Translation*]

Senator Dagenais: Do you find that the policies are effective enough or do they overstate things?

[*English*]

Mr. Geist: I suppose you'd have to look at each individual provider's terms. From what I've seen, and perhaps Professor Slane can expand, they mirror one another fairly closely in terms of the power that an ISP reserves for itself, in terms of what they see as appropriate or inappropriate behaviour on their network.

Do they have the power to address those issues from a contractual perspective? I suspect the answer is yes, but clearly that doesn't provide us with a whole solution to the issue of cyberbullying.

I don't know that anyone seriously is against the cyberbullying-related provisions here. This helps to deal with the issue. I've got three kids who are in school right now. If they were the target of this, I would want to ensure that there are some appropriate rules in place, too.

The problem, in a sense, with a lot of this discussion is that we're talking about two bills. We're talking about a three-page cyberbullying bill and a 40-odd page lawful privacy access bill. We should be having two different conversations about that, and I think we probably could have ensured that we quickly got a very good cyberbullying bill and probably would have got a better lawful access bill as well, especially one that is compliant with *Spencer*, but we have what we have.

Senator Baker: In the *Spencer* case the police used that letter of request under section 7 of PIPEDA. One wonders what is now going to happen to the act, PIPEDA, that's presently on the books. It would apply to Shaw, which I think was the service provider in the *Spencer* case. It wouldn't apply to some other service providers that are not really regulated. If you're looking for privacy, for example, SaskTel would operate as a service provider; they would come under the provincial privacy act of the province.

Cette question a été soulevée dans l'affaire *Spencer*, dans laquelle on a fait valoir que d'une certaine façon, les gens n'ont pas d'attente raisonnable de protection en matière de vie privée parce que les fournisseurs de services Internet essaient de limiter leurs attentes avec ces modalités. La cour a rejeté cet argument parce qu'il ne lui semblait pas raisonnable de conclure que la personne n'avait plus d'attente raisonnable de protection en matière de vie privée sous prétexte qu'elle y aurait renoncé en signant ce contrat.

[*Français*]

Le sénateur Dagenais : Vous trouvez que ces politiques sont assez efficaces ou qu'elles en font trop?

[*Traduction*]

M. Geist : Je suppose qu'il faudrait analyser les modalités de chaque fournisseur de services. D'après ce que j'ai vu, et peut-être Mme Slane pourra-t-elle en parler davantage, ils se réservent tous à peu près les mêmes pouvoirs pour ce qui est de juger des comportements qu'ils estiment appropriés ou non sur leurs réseaux.

Ont-ils le pouvoir de s'attaquer à ces problèmes sur le plan contractuel? Je présume que la réponse est oui, mais cela ne constitue clairement pas de solution complète au problème de la cyberintimidation.

Il n'y a personne à ma connaissance qui soit vraiment contre les dispositions sur la cyberintimidation qu'on trouve ici. Elles contribuent à lutter contre le phénomène. J'ai moi-même trois enfants à l'école. S'ils étaient la cible de cyberintimidation, je voudrais moi aussi qu'il y ait des règles convenables en place.

D'une certaine façon, le problème dans cette discussion, c'est qu'il y a deux projets de loi qui interviennent ici. Il y a le projet de loi de trois pages sur la cyberintimidation et le projet de loi d'environ 40 pages sur l'accès légitime à des renseignements personnels. Nous devrions donc avoir deux conversations différentes à ce sujet, et je crois que nous aurions probablement pu nous organiser pour avoir rapidement un excellent projet de loi sur la cyberintimidation et probablement aussi un meilleur projet de loi sur l'accès légitime à des renseignements personnels, qui serait conforme avec le jugement *Spencer*, mais nous avons ce que nous avons.

Le sénateur Baker : Dans l'affaire *Spencer*, les services de police ont utilisé la lettre de demande prescrite à l'article 7 de la LPRPDE. On peut se demander ce qu'il va advenir de cette loi, la LPRPDE, qu'on prévoit réviser. Elle s'appliquerait à Shaw, qui était le fournisseur de services dans l'affaire *Spencer*, si je ne me trompe pas. Elle ne s'appliquerait pas à d'autres fournisseurs de services qui ne sont pas vraiment réglementés. Du point de vue de la protection des renseignements personnels, SaskTel serait considéré comme un fournisseur de services, mais serait assujetti à la loi de la province sur la protection des renseignements personnels.

Let me ask you one final question, Professor Geist. You're quoted quite often in case law and as time passes, sometimes you may not agree with the quotations that are used. This past year I was just looking at *R. v. Mills*, a Newfoundland and Labrador case. David Orr was the judge. One sentence from paragraph 24 says:

> Counsel for the Crown has argued that there is no expectation of privacy in an email message. She has noted author Michael Geist's book *Internet Law in Canada*, 2nd Edition . . . at page 262:
>
> > You will never hear it enough: e-mail on the Internet is as private and secure as a postcard in the "snail mail". Everyone from your Internet provider staff to your correspondent's friends or colleagues can read your electronic message from the moment you click "SEND" on your computer.

So your book of 2001 was used to say that there's no privacy on the Internet. Do you still hold these comments as being fact?

Mr. Geist: I wasn't aware of that case. I'm tempted to say maybe that's why there's a third edition.

In a sense, we're talking there about two different things. We're talking closer to what Senator Frum was talking about and what the average user feels about the kind of privacy they have when they engage in online activity. I think it is the case that for a lot of users, and certainly in a post-Snowden environment, that's accurate. We learned through Snowden, in a world in which security intelligence agencies are hoovering up all of that information, that the notion that somehow those emails are private is wrong. That just doesn't happen.

But that's not really what is at stake or at issue here. At issue isn't whether or not emails themselves can get captured in a myriad of different ways unless you take steps to encrypt them to provide some level of privacy over those messages. The issue is the standards that we establish in terms of when law enforcement can obtain that under a search and then use that information. That's something quite different.

Senator Baker: *Spencer* was not by a warrant. Let's not be confused here. It was by a letter. There was no warrant. There was no judicial authorization. Under this bill, it provides for judicial authorization in certain circumstances. Yes, based on a suspicion, but it is judicial authorization on a reasonable suspicion basis. So they are two completely different things.

Permettez-moi de vous poser une dernière question, monsieur Geist. Vous êtes très souvent cité dans la jurisprudence, mais il pourrait parfois arriver que vous ne soyez pas d'accord avec les façons dont vous l'êtes. Au cours de la dernière année, j'ai examiné la décision rendue à Terre-Neuve-et-Labrador, dans l'affaire *R c. Mills,* par le juge David Orr. On trouve cette phrase au paragraphe 24 :

> La procureure de la Couronne soutient qu'il n'y pas d'attente en matière de protection de la vie privée lorsqu'un message est envoyé par courriel. Elle cite le livre de l'auteur Michael Geist *Internet Law in Canada,* 2e édition, page 262 :
>
> > On ne l'entendra jamais assez : un courriel dans l'Internet est aussi privé et sécuritaire qu'une carte postale envoyée par courrier ordinaire. N'importe qui, du personnel de votre fournisseur de services Internet jusqu'aux amis et aux collègues de votre correspondant, peut lire votre message électronique dès le moment où vous cliquez sur le bouton « envoyer » de votre ordinateur.

Elle utilise donc votre ouvrage de 2001 pour affirmer qu'il n'y a pas de protection de la vie privée sur Internet. Considérez-vous toujours ces observations véridiques?

M. Geist : Je n'étais pas au courant de ce jugement. Je serais tenté de dire que c'est peut-être la raison pour laquelle il y a une troisième édition.

D'une certaine façon, on parle ici de deux choses différentes. On se rapproche des propos de la sénatrice Frum et de ce que l'utilisateur moyen pense de la confidentialité de ses activités en ligne. Je crois qu'il est vrai que pour beaucoup d'utilisateurs, surtout à l'ère de l'après-Snowden, il n'y en a pas beaucoup. Nous avons appris grâce à l'affaire Snowden qu'il est faux de croire que les courriels sont privés dans un monde où les services du renseignement de sécurité siphonnent toute l'information. Ce n'est tout simplement pas vrai.

Mais ce n'est pas vraiment ce qui est en jeu ici. La question ne consiste pas à savoir si oui ou non, les courriels peuvent être interceptés d'une multitude de façons, à moins que la personne ne prenne de mesures particulières pour les encrypter et les rendre secrets. On se questionne ici plutôt sur les normes qui établissent quand les organismes d'application de la loi peuvent les obtenir grâce à un mandat de perquisition, puis les utiliser. C'est assez différent.

Le sénateur Baker : L'information n'a pas été obtenue par mandat dans l'affaire *Spencer*. Il ne faut pas confondre les choses. Il n'y a eu qu'une lettre, pas de mandat. Il n'y a pas eu d'autorisation judiciaire. Ce projet de loi prévoit d'accorder une autorisation judiciaire dans certaines circonstances. Il faut certes qu'il y ait des soupçons à la base, mais la cour peut accorder une autorisation judiciaire s'il y a des motifs raisonnables de soupçonner quelque chose. Ce sont donc deux choses totalement différentes.

Do you agree with the previous witnesses from the Criminal Lawyers' Association that this will not survive a Charter challenge because of the Supreme Court of Canada's decision in *Spencer*?

Mr. Geist: I don't think there any doubt that it's vulnerable. We talked about voluntary disclosure being clearly vulnerable; that's what we see directly in the *Spencer* case.

On the issue of transmission data, when we look at what the court has said quite consistently, whether in *Vu* or *Spencer* and now some other cases, the *TELUS* case, I think they have coalesced around a view of the privacy import of digital data, so much of the electronic information that is generated when we communicate in these networks. It has recognized that for the law to keep pace we need to be thinking about much of that kind of data in the same way that we thought about content a decade or two ago.

Senator Joyal: There is something that has to be very well understood by everybody. There is no such thing as a presumption that once you are on the computer it's for the whole world to see or read what you do. Senator Frum's question was more or less on the assumption that as long as you dial up on our computer to access your Facebook or you exchange messages, since everybody has a computer and everybody could have access to your computer, then you have no more protection. You have yielded your protection to privacy. That presumption, in my opinion, has been set aside in *Spencer*. The court has been very clear. It's not because you are sitting at your computer that the presumption is that it's for everybody to see.

Of course, your service provider can have a program that, for instance, watches your purchases on eBay, and after a while you have purchases of skis so many times, then you receive all kinds of publicity related to ski resorts and tickets to go there. We know that they have those kinds of programs. But it's not because we see that on our screen that individually we have abandoned our right to privacy. The danger I see in this legislation is once you do that for some kind of objective, the government will find any other kind of objectives to follow the path that is enshrined in this bill. That's what concerns me.

For the sake of the good we will find a lot of other "goods" whereby the threshold to maintain privacy will be lowered. That's my preoccupation. It's in the long term, because I can imagine a lot of other objectives I could propose to you whereby you say that for the sake of national security or radicalization — I could give you a list and I'm sure you could invent one also, and then we will be caught in a different trend of the protection we should have when we use that technology.

Seriez-vous d'accord avec les témoins précédents de la Criminal Lawyers' Association, selon qui ces dispositions ne survivraient pas à une contestation sur la base de la Charte en raison de la décision que la Cour suprême du Canada a rendue dans l'affaire *Spencer*?

M. Geist : Je pense qu'il ne fait aucun doute qu'il y a là une vulnérabilité. Nous avons déjà dit que la divulgation volontaire comportait clairement sa part de vulnérabilité : c'est ce qu'on constate directement dans l'affaire *Spencer*.

Au sujet des données de transmission, quand on regarde ce que les juges ont dit et répété dans bien des décisions, dans les affaires *Vu*, *Spencer* et d'autres comme celle de *TELUS*, ils semblent assez unanimes sur le caractère confidentiel des données numériques et d'une grande partie de l'information électronique que nous générons lorsque nous communiquons à l'aide de ces réseaux. Les tribunaux reconnaissent qu'en droit moderne, il faut voir ce type de données un peu comme on voyait le contenu il y a 10 ou 20 ans.

Le sénateur Joyal : Il y a une chose que tout le monde doit très bien comprendre. On ne peut pas présumer que dès qu'une personne fait quelque chose sur un ordinateur, tout le monde peut le lire ou le voir. La question de la sénatrice Frum se fondait surtout sur l'hypothèse selon laquelle dès qu'on accède à son compte Facebook ou à ses messages Exchange de son ordinateur, on n'est plus protégé, puisque tout le monde a un ordinateur et peut avoir accès à un autre ordinateur de nos jours. On se trouverait alors à renoncer à la protection de ses renseignements personnels. À mon avis, le jugement *Spencer* réfute bien cette hypothèse. Le tribunal a été très clair. Ce n'est pas parce qu'on fait quelque chose sur un ordinateur que tout le monde peut s'attendre à y avoir accès.

Bien sûr, votre fournisseur de services peut avoir un programme qui lui permet, par exemple, de surveiller vos achats sur eBay, de sorte qu'après avoir acheté des skis tant de fois, vous receviez toutes sortes de publicités sur les centres de ski et les billets pour y aller. Nous savons qu'ils ont ce genre de programmes, mais ce n'est pas parce que nous les voyons sur nos écrans radars que nous avons abandonné notre droit à la vie privée individuellement. Le danger que je vois dans ce projet de loi, c'est qu'à partir du moment où on le permet pour un certain objectif, le gouvernement va trouver le moyen de faire suivre la même voie à d'autres objectifs. C'est ce qui m'inquiète.

On va trouver toutes sortes d'autres « bonnes raisons » d'abaisser le seuil de protection des renseignements personnels. C'est ce qui me préoccupe. C'est une perspective à long terme, parce que je peux imaginer bien d'autres objectifs qui vous sembleraient très louables pour protéger la sécurité nationale ou prévenir la radicalisation : je pourrais vous en donner une liste et je suis certain que vous pourriez en dresser une vous aussi, mais nous risquerions alors d'être pris dans une autre tendance de protection que celle que nous devrions mettre de l'avant pour l'utilisation de ces technologies.

Mr. Geist: Our country and other countries have created specific privacy rules that someone shouldn't know what books I read or take out of the library. This is my library. We have rules in the U.S., after the Bork hearings, which talk about privacy protection for people's video rental activities because people shouldn't necessarily get access to what we watch. This is my video store. This single device functions in so many different ways. For some reason we've recognized in the past, over the course of a couple of decades, about the privacy importance in that off-line environment and we're about to pass legislation that hasn't kept pace with how these kinds of devices generate all that same information but perhaps without the same level of protection that we've almost now taken for granted in an off-line or non-digital environment.

Senator Baker: Mr. Geist, you heard of the case called *TELUS v. R.*, Supreme Court of Canada, not long ago. The Supreme Court of Canada approved the standard of 487.012, which is a judge's belief on reasonable grounds that an officer has a suspicion to obtain. The majority of the court — Justice Cromwell disagreed, probably right in my opinion — agreed that you could on a suspicion, on that section, obtain what existed in *TELUS*, which was your text messaging, and so on, that they kept for a 30-day period as an exception to 186 for quality control purposes. Do you think now the Supreme Court of Canada will reverse their position on that given what they've now decided in *Spencer*?

Mr. Geist: No. The *TELUS* decision is close enough in time that they won't.

What I take away from the *TELUS* case are a couple of things. First is how rare it is for a telecom provider to go to bat for their subscriber information in these contexts. The *TELUS* case notable because so few telecom companies have done anything to stand up to attempts to access this kind of information, which is why it's notable in its own right, and secondarily, for the court to begin to grapple with that notion of interception and storage and recognize that there are differences.

We've got a court that's willing to truly examine the technology and think about what that means from a privacy perspective. In that case we had at least one telecom company willing to do the same. The fear is, especially from the telecom perspective, they are a bit of an outlier when it comes to that willingness to stand up for customer privacy.

Senator Joyal: What is the situation in the United States in relation to the same issue?

M. Geist : Le Canada comme d'autres pays s'est doté de règles de protection de la vie privée selon lesquelles personne ne devrait savoir quels livres je lis ou j'emprunte à la bibliothèque. Ce sont mes choix de lecture. Il y a des règles aux États-Unis, depuis les audiences *Bork*, qui assurent la protection de la confidentialité des activités de location de vidéos des gens, parce que les autres ne doivent pas nécessairement avoir accès à la liste de tout ce qu'une personne regarde. Ce sont mes choix vidéo. Ce mécanisme peut fonctionner de tellement de façons différentes. Pour diverses raisons, nous avons reconnu par le passé, pendant quelques décennies, l'importance de protéger les renseignements personnels dans l'environnement hors ligne, mais nous nous apprêtons à adopter une loi qui ne tient pas compte du fait que ces outils génèrent le même genre de renseignements, sans toutefois bénéficier du même degré de protection, une protection que nous tenons presque pour acquise dans l'environnement hors ligne ou non numérique.

Le sénateur Baker : Monsieur Geist, vous avez entendu parler de l'affaire *TELUS c. R.*, qu'a entendue la Cour suprême du Canada il n'y a pas si longtemps. La Cour suprême du Canada a approuvé la norme établie par l'article 487.012, qui habilite un juge à déterminer qu'un agent de la paix a des motifs raisonnables d'obtenir un mandat en raison de soupçons. La majorité des juges (le juge Cromwell a signifié sa dissidence, probablement à juste titre à mon avis) que cet article permettait, sur la base de doutes raisonnables, d'obtenir les renseignements visés par l'affaire *TELUS*, c'est-à-dire les messages textes d'une personne et les autres renseignements que l'entreprise conservait pour une période de 30 jours, par exemption à l'article 186, pour le contrôle de la qualité des services. Croyez-vous que la Cour suprême du Canada va changer sa position compte tenu de la décision qu'elle a rendue dans l'affaire *Spencer*?

M. Geist : Non. L'arrêt *TELUS* est trop récent.

Je retiens toutefois un certain nombre de choses de cet arrêt. D'abord, il est extrêmement rare qu'un fournisseur de services de télécommunications se batte pour les renseignements sur ses abonnés dans ce genre de contexte. L'affaire *TELUS* est remarquable parce qu'il y a très peu d'entreprises de télécommunication qui se battent pour lutter contre les tentatives d'accès à ces renseignements, ce qui mérite déjà d'être souligné, mais il est aussi remarquable que la cour commence à définir les notions d'interception et de conservation et à reconnaître qu'il y a des différences entre les deux.

La Cour suprême semble véritablement déterminée à se pencher sur la technologie et à réfléchir à la protection de la vie privée dans ce contexte. Dans ce cas-ci, il y avait au moins une société de télécommunications prête à en faire autant. La plus grande crainte, c'est que les sociétés de télécommunication, particulièrement, n'aient pas trop envie de se battre pour protéger la vie privée des consommateurs.

Le sénateur Joyal : Quelle est la situation aux États-Unis à cet égard?

Mr. Geist: In some ways, if we look at what we've seen in the post-Snowden environment, the U.S. is highly instructive about what not to do as opposed to what to do. I think we could look at the level of surveillance that exists in that jurisdiction. We're part of the Five Eyes, so we're playing along with all of that. But the expectation of privacy there is lower even than it would be here, and part of that stems from the fact that they don't even have basic national privacy legislation. The one exception to that — the exception to the exception, I guess — is the *Fearon* case, which is this issue of accessing information on a cellphone that isn't password protected. That's a case that the U.S. Supreme Court heard and has decided and our own Supreme Court has heard a very similar case and will render a decision very soon, and the U.S. court ruled that there was privacy in that information. I suspect our court will follow suit.

The Chair: Witnesses, thank you very much for a most interesting contribution to our deliberations. It's much appreciated.

Members, we will meet again tomorrow morning to continue our study of Bill C-13.

(The committee adjourned.)

OTTAWA, Thursday, November 20, 2014

The Standing Senate Committee on Legal and Constitutional Affairs, to which was referred Bill C-13, An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act, met this day at 10:30 a.m. to give consideration to the bill.

Senator Bob Runciman (*Chair*) in the chair.

[*English*]

The Chair: Welcome, colleagues, invited guests, and members of the general public who are following today's proceedings of the Standing Senate Committee on Legal and Constitutional Affairs.

We are meeting today to continue our study of Bill C-13, An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act. As a reminder to those watching, these committee hearings are open to the public and also available via webcast on the parl.gc.ca website. You can find more information on the schedule of witnesses, on that same website, under "Senate Committees."

M. Geist : D'une certaine façon, si l'on analyse la situation à la suite de l'affaire Snowden, on voit que les États-Unis se dotent de beaucoup de directives sur ce qu'il ne faut pas faire plutôt que sur ce qu'il faut faire. Je pense que nous pourrions examiner la surveillance qui s'exerce dans ce pays. Nous faisons partie du Groupe des Cinq, nous faisons donc partie du système. Mais les attentes en matière de protection de la vie privée y sont bien inférieures à ce qu'elles sont ici, notamment parce qu'il n'y a pas là-bas de loi nationale qui protège la vie privée à la base. La seule exception — et c'est probablement l'exception à l'exception — est celle de l'affaire *Fearon*, qui porte sur l'accès à l'information détenue sur un téléphone cellulaire non protégé par un mot de passe. La Cour suprême des États-Unis a rendu une décision dans cette affaire, et notre propre Cour suprême a entendu une affaire très semblable sur laquelle elle va rendre une décision très bientôt. La cour américaine a statué que ces renseignements avaient un caractère privé. Je m'attends à ce que notre propre Cour suprême fasse de même.

Le président : Chers témoins, je vous remercie infiniment de cette contribution extrêmement intéressante à nos délibérations. Nous vous en sommes très reconnaissants.

Mesdames et messieurs les sénateurs, nous allons nous réunir de nouveau demain matin, pour continuer notre étude du projet de loi C-13.

(La séance est levée.)

OTTAWA, le jeudi 20 novembre 2014

Le Comité sénatorial permanent des affaires juridiques et constitutionnelles, auquel a été renvoyé le 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 se réunit aujourd'hui, à 10 h 30, pour étudier le projet de loi.

Le sénateur Bob Runciman (*président*) occupe le fauteuil.

[*Traduction*]

Le président : Je souhaite la bienvenue aux sénateurs, aux invités et aux membres du grand public qui suivent aujourd'hui les délibérations du Comité sénatorial permanent des affaires juridiques et constitutionnelles.

Nous sommes réunis aujourd'hui pour poursuivre 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. Je rappelle à nos téléspectateurs que les audiences du comité sont ouvertes au public et qu'elles sont aussi diffusées sur le site web parl.gc.ca. Vous trouverez de plus amples renseignements sur le calendrier de comparution des témoins sur le même site web, sous la rubrique « Comités du Sénat ».

We welcome, from the Canadian Bar Association, Tony Paisana, Executive Member, Criminal Justice Section. He is appearing via video conference from Vancouver, British Columbia. Welcome, sir. Do you have an opening statement?

Tony Paisana, Executive Member, Criminal Justice Section, Canadian Bar Association: Yes, I do. Thank you for the invitation to present the Canadian Bar Association's views on Bill C-13. The CBA is a national association of over 37,500 lawyers, students, notaries and academics. An important aspect of our mandate is seeking improvements in the law and the administration of justice. It's that aspect of our mandate that brings us to you today.

Our submission on Bill C-13 was a joint effort led by our national criminal justice section, with input from our privacy and access to information law section, our competition law section, as well as our children's law committee.

I am an executive member of the national criminal justice section, which represents a balance of both Crown and defence counsel from all parts of the country. Personally, I practise predominantly in criminal defence, in Vancouver, but from time to time I also practise as a Crown lawyer.

We have prepared a 25-page written submission summarizing our views on the two main aspects of Bill C-13. They are the cyberbullying offence on the one hand and the lawful access provisions on the other.

Our submission includes 19 recommendations. In my brief opening statement, I will not be able to comment on all of those recommendations, but they are set out in the submission for your consideration and review.

I hope to focus on two overall themes prevalent in our submission. The first is that we suggest refining the cyberbullying offence, section 162.1, so that it captures only truly intentional cyberbullying conduct, as is the apparent intention of Parliament. Second, we offer suggestions to improve the lawful access provisions to ensure privacy is protected to the maximum extent while still allowing for the effective and responsive investigation of crime.

I will first deal with the proposed cyberbullying offence. The CBA welcomes and supports the inclusion of this offence in the Criminal Code. The section directly criminalizes harmful conduct that was otherwise difficult to capture with older, outdated provisions.

The section also provides a prudent alternative to the child pornography offences, which were sometimes utilized in the cyberbullying context but with, we say, disproportionate effect, at points.

Nous accueillons Tony Paisana, membre de l'exécutif, Section du droit pénal, de l'Association du Barreau canadien. Il comparaît par vidéoconférence de Vancouver, en Colombie-Britannique. Bonjour, monsieur. Avez-vous une déclaration préliminaire?

Tony Paisana, membre de l'exécutif, Section du droit pénal, Association du Barreau canadien : Oui, j'en ai une. Merci d'avoir invité l'Association du Barreau canadien à présenter ses points de vue sur le projet de loi C-13. L'ABC est une association nationale réunissant plus de 37 500 avocats, étudiants, notaires et universitaires. Un des aspects importants de notre mandat consiste à trouver des façons d'améliorer la loi et l'administration de la justice. C'est cet aspect de notre mandat qui nous amène ici aujourd'hui.

Notre mémoire sur le projet de loi C-13 est le fruit d'un effort conjoint mené par la Section nationale du droit pénal, avec des commentaires de la Section nationale du droit à la vie privée, de la Section nationale du droit à la concurrence et du Comité du droit des enfants.

Je suis un membre de l'exécutif de la Section nationale du droit pénal, qui représente autant des avocats de la Couronne que des avocats de la défense de partout au pays. Personnellement, j'ai principalement œuvré à titre d'avocat criminaliste, à Vancouver, mais, de temps à autre, j'ai aussi occupé le poste de procureur de la Couronne.

Nous avons préparé un mémoire de 25 pages qui résume nos points de vue sur les deux principaux aspects du projet de loi C-13, soit, d'un côté, l'infraction de cyberintimidation, et de l'autre, les dispositions sur l'accès légal.

Notre mémoire compte 19 recommandations. Dans ma brève déclaration préliminaire, je ne pourrai pas revenir sur l'ensemble de ces recommandations, mais elles sont expliquées dans le mémoire, où vous pourrez les consulter et les examiner.

Je veux me concentrer sur deux thèmes généraux importants dans notre mémoire. Le premier, c'est que nous suggérons de préciser l'infraction de cyberintimidation, l'article 162.1, afin qu'il englobe seulement les cas de cyberintimidation vraiment intentionnels, puisque ce semble être l'intention du Parlement. Deuxièmement, nous formulons des suggestions pour améliorer les dispositions sur l'accès légal afin de garantir le plus possible la protection des renseignements personnels tout en permettant la tenue d'enquêtes efficaces et rapides en cas de crime.

Je vais commencer par l'infraction de cyberintimidation proposée. L'ABC salue et appuie l'inclusion de cette infraction dans le Code criminel. Cet article criminalise directement un comportement néfaste qui, autrement, était difficile à cibler avec les anciennes dispositions périmées.

Cet article offre aussi une solution de rechange prudente aux infractions de pornographie infantile, qui étaient parfois utilisées dans des dossiers de cyberintimidation, mais qui, selon nous, étaient, dans certains cas, disproportionnées.

The CBA suggests two narrow but important revisions to the section to ensure it captures the conduct we normally associate with cyberbullying, as opposed to careless distribution of intimate images without the criminal intent we normally associate with cyberbullying.

This offence was introduced by the Minister of Justice as an effort "to put an end to harmful online harassment and exploitation." The honourable minister specifically referred to the term "cyberbullying", although that term does not appear in the text of the offence. "Cyberbullying" has a specific meaning. The CCSO Cybercrime Working Group, whose report was heavily relied upon by the government in formulating this offence, defines cyberbullying as "the use of information and communication technologies that support deliberate, hostile, and often repeated behaviour by an individual or group that is intended to hurt others."

Critically, in our submission, this definition includes specific reference to deliberate and intentional conduct or what we sometimes refer to as specific intent. However, two aspects of the cyberbullying offence appear to criminalize conduct which may lack this specific intent.

First, the section is broadly worded to capture any sharing of images without consent, making no reference to the purpose of the distribution. This broad wording conceivably captures conduct which is removed from the deliberate and harmful conduct that we associate with cyberbullying. We provide an example of this problem in our hypothetical fact pattern, on page 5 of our submission.

To remedy this issue, we recommend a specific intent be built into the offence. What we have suggested is that the wording "with the intent to annoy, embarrass, intimidate or harass" be added to the provision.

The second revision we suggest is removing the recklessness standard from the *mens rea*, or mental element, of the offence. Given the practical reality of the Internet, there is a potentially wide sliding scale of moral culpability in the distribution of intimate images. Truly intentional cyberbullying refers to those who have direct knowledge of the source of an image and distribute it with that malicious intent. By including the recklessness standard, the section criminalizes individuals who may have little to no knowledge of the origins of an image, who is depicted in it, and perhaps most importantly, the intent behind its original distribution.

In our submission, the criminal law is a blunt tool that has lifelong impacts on those who are implicated within its scope. It should only be employed when absolutely necessary and in

L'ABC suggère deux légères modifications qu'elle juge tout de même importantes à l'article, afin de s'assurer qu'il englobe les comportements que nous associons habituellement à la cyberintimidation, et non la distribution par inadvertance d'images intimes sans l'intention criminelle que nous n'y associons habituellement pas.

Cette infraction a été présentée par le ministre de la Justice dans un effort pour « mettre fin au harcèlement et à l'exploitation nuisibles en ligne ». Le ministre a utilisé précisément le terme « cyberintimidation », même si ce terme ne figure pas dans le libellé dans l'infraction. La notion de « cyberintimidation » a une signification précise. Pour formuler l'infraction de cyberintimidation, le gouvernement s'est beaucoup appuyé sur le rapport du Groupe de travail sur la cybercriminalité du CCHF, qui définit la cyberintimidation comme suit : « l'utilisation des technologies de l'information et des communications qui facilitent le comportement délibéré, hostile et souvent répété d'une personne ou d'un groupe dans l'intention de faire du mal à d'autres. »

Dans notre mémoire, nous soulignons que cette définition fait directement référence à un comportement délibéré et intentionnel, ou ce qu'on appelle parfois une intention particulière. Cependant, deux aspects du libellé de l'infraction de cyberintimidation semblent criminaliser un comportement qui n'est peut-être pas associé à cette intention particulière.

Premièrement, le libellé de l'article est général et il englobe ainsi tout partage d'images sans consentement sans mention de l'objectif de la distribution. On peut concevoir que ce libellé général est susceptible d'englober des comportements qui n'ont rien à voir avec le comportement délibéré et préjudiciable que nous associons à la cyberintimidation. Nous avons fourni un exemple de ce problème, appliqué à une situation hypothétique, à la page 5 de notre mémoire.

Pour corriger ce problème, nous recommandons d'inclure une intention particulière dans le libellé de l'infraction. Nous avons suggéré d'ajouter le libellé suivant à l'article : « avec l'intention de contrarier, d'embarrasser, d'intimider ou de harceler cette personne ».

La deuxième modification que nous suggérons est d'éliminer la norme d'insouciance de l'intention coupable, ou de l'élément psychologique de l'infraction. Compte tenu de la réalité d'Internet, il y a potentiellement tout un spectre de culpabilité morale liée à la distribution d'images intimes. La cyberintimidation véritable est commise par ceux qui connaissent directement la source d'une image et la distribuent de façon malveillante. En incluant la norme d'insouciance, l'article criminalise des personnes qui, peut-être, connaissent peu ou pas l'origine d'une image, qui elle représente et, ce qui est peut-être encore plus important, l'intention visée au moment de sa distribution initiale.

Selon nous, le droit pénal est un outil grossier qui peut avoir des répercussions permanentes sur les personnes qui ont des démêlés avec le système. Il faut seulement y avoir recours lorsqu'il

accordance with the stated objectives of each piece of legislation. In this case, Parliament has introduced this legislation to combat harassing and exploitive conduct which carries a specific intent. The recklessness standard broadens the scope of this provision beyond its intended target and raises constitutional concerns of over-breadth in that respect.

Dealing with the lawful access of the bill, on page 11 we begin to make a series of recommendations with respect to that aspect of the bill.

With respect to the preservation demand, section 487.012, we make four specific recommendations. The first is that this preservation power be conferred to an officer only in exigent circumstances where there is reason to believe that the data in question may be lost. Second, we recommend a shorter period of preservation — it's currently 21 days — to make it more consistent with the urgent nature of these requests. Third, we recommend eliminating officer-created conditions on these demands as they lack judicial oversight but nonetheless carry potential criminal penalty. Fourth, we recommend that this power, along with the preservation order in 487.013, be limited to the investigation of offences under Canadian law or offences under foreign law which have equivalents within the Canadian law.

Finally, with respect to the production orders in section 487.016 — that relates to transmission data — we recommend that the standard be increased from "reasonable grounds to suspect" to "reasonable grounds to believe." We make the same recommendation with respect to warrants for transmission data recorders, and that's section 492.2.

In our submission, this position recognizes the sensitive nature of transmission data and recent pronouncements from the Supreme Court of Canada about the protection of privacy and anonymity in the modern age. Thank you.

The Chair: We will begin the questions with the committee's deputy chair, Senator Baker.

Senator Baker: Thank you, witness, for your presentation. I'm glad you cleared up the matter of whether or not you represent the Crown or defence attorney. I noticed in case law, from time to time, you represented both. You go back and forth. So you see both sides of the picture.

On the question, we've heard a great deal from witnesses from the legal community who question the grounds, as you have, of reasonable suspicion. I happen to know that you've litigated this matter of what is a reasonable suspicion. To support your

est absolument nécessaire de le faire et conformément aux objectifs énoncés de chaque loi. Dans ce cas, le Parlement a produit le projet de loi pour lutter contre des comportements de harcèlement et d'exploitation ayant une intention particulière. La norme d'insouciance élargit la portée de cette disposition au-delà de l'intention initiale, et peut soulever des préoccupations constitutionnelles liées à sa trop grande portée à cet égard.

En ce qui concerne le thème de l'accès légal dans le projet de loi, à la page 13 du mémoire, nous avons formulé une série de recommandations relativement à cet aspect du projet de loi.

En ce qui concerne l'ordre de préservation, à l'article 487.012, nous formulons quatre recommandations précises. La première, c'est qu'il faut uniquement conférer le pouvoir de donner un ordre de préservation à un agent dans les cas d'urgence où il y a des raisons de croire que les données en question pourraient être perdues. Deuxièmement, nous recommandons de raccourcir la période de préservation — qui est actuellement de 21 jours — pour qu'elle corresponde davantage à la nature urgente de ces demandes. Troisièmement, nous recommandons l'élimination des conditions imposées par les agents dans le cadre de ces demandes parce qu'elles font l'objet d'aucune surveillance judiciaire, mais peuvent tout de même entraîner des sanctions pénales. Quatrièmement, nous recommandons que ce pouvoir, ainsi que le pouvoir relatif aux ordonnances de préservation de l'article 487.013, soient limités aux enquêtes relativement à la perpétration d'une infraction criminelle à une loi fédérale ou à la perpétration d'une infraction criminelle à la loi d'un État étranger qui constituerait également un crime au Canada.

Enfin, en ce qui concerne les ordonnances de communication aux termes de l'article 487.016 — qui porte sur les données de transmission —, nous recommandons d'accroître la norme, pour qu'elle passe de « motifs raisonnables de soupçonner » à des « motifs raisonnables de croire ». Nous formulons la même recommandation en ce qui concerne les mandats pour les enregistreurs de données de transmission, à l'article 492.2.

Selon nous, cette position tient compte de la nature délicate des données de transmission et des récentes décisions de la Cour suprême du Canada au sujet de la protection de la confidentialité et de l'anonymat à l'ère moderne. Merci.

Le président : Nous allons passer aux questions, et commencer par le vice-président du comité, le sénateur Baker.

Le sénateur Baker : Je remercie le témoin de son exposé. Je suis heureux que vous ayez fait la lumière sur la question de savoir si vous représentez les avocats de la Couronne ou de la défense. J'ai constaté dans la jurisprudence que, de temps à autre, vous avez assumé les deux rôles. Vous passez d'un rôle à l'autre, alors vous avez vu ce qui se passe des deux côtés.

Nous avons entendu beaucoup de témoins du milieu juridique qui remettent en question les motifs, tout comme vous, du soupçon raisonnable. Je sais que vous avez plaidé au sujet de la signification de soupçons raisonnables. Pour appuyer votre

argument, you used the Supreme Court of Canada decision in *Mann*, in which a reasonable suspicion has not only a subjective element but also an objective element.

Under our present law, reasonable suspicion is what grounds a production order for financial statements under the Criminal Code, for production orders under the Criminal Code today. Since it does have an objective and subjective element composed in it — in other words, it's not just somebody suspects, it's reasonable grounds to suspect — both elements — why would somebody say that is insufficient to ground the warrants that are being given under this legislation?

Mr. Paisana: Thank you for your question, senator.

The difference between the two is fairly wide, in our respectful view. The decision of *Chehil* out of the Supreme Court of Canada from 2013 provides some useful guidance on the difference between the two. Put simply, it's the difference between reasonable possibility on the one hand and a reasonable probability on the other. Reasonable suspicion is posited somewhere in between a mere hunch and reasonable grounds to believe.

Because of this lower threshold, the Supreme Court of Canada explicitly recognizes in *Chehil* that you will capture innocent persons as a result of this lower standard, as it will necessarily involve conduct that can apply to a wide range of individuals. The example in that case was when we go to the airport and you're asked questions about your luggage and appearing nervous, as opposed to an example where there may be the smell of marijuana clearly emanating from your luggage. Those two sets of scenarios provide a very different standard of reasonable grounds, one providing for a much more limited search and the second providing for a much more intrusive search.

In the context of the Protecting Canadians from Online Crime Bill, it is our view that the higher standard should be applied with respect to pieces of information that can reveal information about an individual which strikes at the biographical core of their being, as that language is sometimes used.

Senator Baker: As a final question to you because time is passing, most of the witnesses before our committee referenced the *Spencer* case, which was brought down after the House of Commons dealt with this bill in committee, by the way. It was in June of this year. However, the Supreme Court of Canada did not deal with reasonable suspicion. They were dealing with a request from the police in writing under PIPEDA, the Personal Information Protection and Electronic Documents Act. So I'm wondering what your view is on the stretch one would be making in saying that the provisions of *Spencer* apply to the provisions that we have under discussion in this bill when the Supreme Court

argument, vous avez utilisé l'arrêt *Mann*, de la Cour suprême du Canada, dans lequel la cour a affirmé qu'un soupçon raisonnable compte non seulement un élément subjectif, mais aussi un élément objectif.

Dans la loi actuelle, on s'appuie sur un soupçon raisonnable pour présenter une ordonnance de communication d'états financiers aux termes du Code criminel, pour les ordonnances de communication aux termes du Code criminel actuel. Puisque ce motif compte un élément objectif et un élément subjectif — en d'autres mots, il ne faut pas seulement soupçonner, il faut avoir des motifs raisonnables de soupçonner, les deux éléments —, pourquoi quelqu'un dirait-il que c'est insuffisant pour justifier les mandats qui sont accordés aux termes de cette loi?

M. Paisana : Merci de poser la question, sénateur.

Nous affirmons respectueusement qu'il y a une assez grande différence entre les deux. Dans son arrêt *Chehil*, de 2013, la Cour suprême du Canada a fourni des directives utiles pour différencier les deux. Dit simplement, c'est la différence entre une possibilité raisonnable d'un côté, et une probabilité raisonnable de l'autre. Le soupçon raisonnable se situe entre une simple intuition et des motifs raisonnables de croire.

En raison de ce seuil plus bas, la Cour suprême du Canada a reconnu explicitement dans l'arrêt *Chehil* qu'on arrêtera des personnes innocentes parce qu'on utilise ce critère plus général, du fait qu'il regroupe des comportements qu'on peut associer à un large éventail de personnes. L'exemple donné dans ce dossier, c'est lorsqu'on va à l'aéroport et qu'on nous pose des questions au sujet de nos bagages et qu'on semble nerveux, comparativement à une situation où l'on constate clairement que les bagages sentent la marijuana. Ces deux scénarios reflètent des applications très différentes des motifs raisonnables, l'un exigeant une fouille beaucoup plus limitée, et l'autre, beaucoup plus intrusive.

Dans le contexte de la Loi sur la protection des Canadiens contre la cybercriminalité, nous estimons qu'il faudrait appliquer une norme plus élevée relativement aux éléments d'information pouvant révéler des renseignements au sujet d'une personne, des renseignements biographiques d'ordre personnel, comme on les appelle parfois.

Le sénateur Baker : Le temps passe, alors j'ai une dernière question pour vous. La plupart des témoins que nous avons rencontrés ont mentionné la décision *Spencer*, qui, en passant, est tombée après que la Chambre des communes avait étudié le projet de loi en comité. C'était en juin, cette année. Cependant, la Cour suprême du Canada ne s'est pas attardée à la question du soupçon raisonnable. Elle portait sur une demande écrite de la police aux termes de la LPRPDE, la Loi sur la protection des renseignements personnels et les documents électroniques. Alors, je me demande si, selon vous, il est raisonnable pour une personne de dire que les dispositions de l'arrêt *Spencer* s'appliquent aux dispositions qui

of Canada passed no judgment whatsoever on the definition of "reasonable suspicion" as far as the warrant is concerned, the judicial application of the law.

Mr. Paisana: Yes. And to be clear, I was referring to the *Chehil* decision earlier, not the *Spencer* decision.

Senator Baker: That is the sniffer dog case.

Mr. Paisana: Yes. With respect to S*pencer*, a few very important things come out of that case and have some implication for this bill. For the first time, the Supreme Court of Canada explicitly recognized that anonymity is an important aspect of privacy. This bill strikes at some of that. What the court also said, which is important in respect to this bill, is that information that tends to reveal — that's the language they use — Internet usage by an individual engages significant privacy interests at the high end of the scale. Therefore, when you consider what they've said about information, which tends to reveal Internet usage, and you marry that up with what *Chehil* says about the difference in standards and why we should appropriate a reasonable-grounds-to-believe standard, the reasonable ground to believe is the more appropriate standard vis-à-vis warrants and production orders on transmission data.

Senator McInnis: Unfortunately, I was not here yesterday when the Criminal Lawyers' Association was here. I would like to have been. The traveller I was with had problems with planes.

In any event, your association has said that Bill C-13 sacrifices privacy in favour of expanded police powers and liberal disclosure standards.

Now, Canadians have clearly told the Government of Canada that they want this harm being inflicted on Canadians through cyberbullying, particularly the youth, to be cured. They want it handled.

I will read your brief, as the sponsor of the bill and as all members of the committee will do, under the technical details, but this government arrived at this legislation first of all through the federal, provincial and territorial ministers of justice in a working group over a long period of time and submitted the report; it's interesting. You're a Crown prosecutor and a criminal lawyer. We've had those practitioners from across the country analyze this piece of legislation. Government prosecutors, which you say you have done on a part-time basis, have come here and they've agreed with it. So has the Canadian Associations of Chiefs of Police, which represents 90 per cent of the police in the country who have lawyers on staff, RCMP, Ontario Provincial Police, interest groups, and Canadians that want this problem handled.

sont à l'étude dans le projet de loi, alors que la Cour suprême du Canada n'a absolument rien dit sur la définition de « soupçon raisonnable » en ce qui concerne les mandats, l'application judiciaire de la loi?

M. Paisana : Oui. En outre, je tiens à préciser que j'ai parlé de l'arrêt *Chehil* tantôt, et non de l'arrêt *Spencer*.

Le sénateur Baker : C'est le cas du chien détecteur.

M. Paisana : Oui. Pour ce qui est de l'arrêt S*pencer*, il y a quelques choses très importantes qui découlent de ce dossier et qui ont une certaine répercussion sur le projet de loi. Pour la première fois, la Cour suprême du Canada a reconnu explicitement que l'anonymat est un aspect important de la vie privée. Le projet de loi en tient compte à certains égards. Ce que la cour a aussi dit, et c'est important en ce qui concerne le projet de loi, c'est que les renseignements qui ont tendance à révéler — c'est le mot qui est utilisé — l'utilisation que fait une personne d'Internet met en jeu d'importants droits en matière de vie privée, à l'extrémité supérieure de l'échelle. Par conséquent, lorsqu'on tient compte de ce que la cour a dit au sujet des renseignements, qui ont tendance à révéler l'utilisation d'Internet, et que vous associez cette position à ce qu'elle a dit dans l'arrêt *Chehil* au sujet de la différence de norme, et pourquoi nous devrions établir la norme des « motifs raisonnables de croire », cette dernière est plus appropriée pour les mandats et les ordonnances de communication touchant les données de transmission.

Le sénateur McInnis : Malheureusement, je n'étais pas ici hier lorsque nous avons accueilli la Criminal Lawyers' Association. J'aurais bien aimé y être. La personne qui m'accompagnait n'aime pas prendre l'avion.

Quoi qu'il en soit, votre association a dit que le projet de loi C-13 sacrifie la vie privée sur l'autel des pouvoirs accrus de la police et de normes plus libérales en matière de divulgation.

Cependant, les Canadiens ont dit clairement au gouvernement du Canada qu'ils veulent qu'on élimine tout le mal qui est infligé aux Canadiens par le truchement de la cyberintimidation, et particulièrement les jeunes. Ils veulent qu'on règle ce dossier.

Je vais lire votre mémoire, en tant que parrain du projet de loi, comme tous les membres du comité le feront, pour reconnaître les détails techniques, mais le gouvernement a produit ce projet de loi, dans un premier temps, grâce au long travail d'un groupe réunissant les ministres de la Justice fédéral, provinciaux et territoriaux, qui a présenté le rapport. C'est intéressant. Vous êtes un procureur de la Couronne et un avocat criminaliste. Nous avons fait analyser le projet de loi par de tels avocats qui pratiquent partout au pays. Des procureurs du gouvernement, rôle que vous avez affirmé avoir joué à temps partiel, sont venus nous voir pour nous dire qu'ils étaient d'accord avec le projet de loi. C'est aussi le cas de l'Association canadienne des chefs de police, qui représente 90 p. 100 des policiers du pays et qui

In my opinion, they all agree, and the committee can judge for themselves reading the briefs that have been submitted. It opens the door for law enforcement to commence an investigation so that they can take a step at a time. To do so, the threshold has been lowered to suspect.

We are told by the experts that if they did not have that initial opportunity using the threshold of suspicion, the investigation probably would not go forward because they do not have sufficient evidence to deal with reasonable belief.

All of these orders that are being given to the police are scrutinized by the judiciary. How is it sacrificing privacy, in favour of expanded police powers, when it is a step at a time used in precision with judicial oversight? How could your association make that comment?

Mr. Paisana: I want to clarify what our submission actually says. Our submission is comprehensive and for the most part is supportive of the bill. Where we've made some narrow recommendations is with respect to transmission data on this topic that you've raised about reasonable suspicion and reasonable belief.

You'll see that we also wholeheartedly accept and support the cyberbullying offence. So I want to make that very clear about our position.

With the ability of the police to investigate, and our submission with respect to these two areas where we say a higher threshold should be implemented, we don't see that it will create an impediment for the types of offences we all are talking about.

You're quite right that the tragic cases we've heard about created an impetus for your government to react, and it has done so. We will support in large measure what has been done, but let's think about the practical example that those cases show us, and that is we have an individual complainant who comes to the police and says someone is sharing an intimate image of me without my consent. Now, under this bill, with the inclusion of the new cyberbullying offence, that will provide clear, reasonable grounds to believe that an offence has been committed. You wouldn't have to resort to the reasonable suspicion standard. You have a complainant who can identify an image and who says that they have not consented to its being shared. That would satisfy the higher threshold easily. It is not an insurmountable threshold.

Where the difference lies is where the fact pattern is such that you don't have clear evidence. It's verging on a mere hunch but barely crosses that threshold into a reasonable suspicion. When you're dealing with sensitive information such as Internet history,

emploie des avocats, la GRC, la Police provinciale de l'Ontario, des groupes d'intérêt et des Canadiens qui veulent que nous réglions ce problème.

Selon moi, ils sont tous d'accord, et les membres du comité pourront en juger par eux-mêmes en lisant les mémoires qui ont été présentés. Le projet de loi permet aux organisations d'application de la loi de commencer une enquête afin qu'elles puissent y aller une étape à la fois. Pour y arriver, le seuil a été réduit aux soupçons.

Des experts nous ont dit que, si on ne leur donne pas, au départ, l'occasion d'utiliser le seuil des soupçons, il n'y aura probablement pas d'enquête parce qu'ils n'auront pas suffisamment d'éléments de preuve pour respecter le critère des motifs raisonnables.

Toutes ces ordonnances qui sont données à la police sont examinées de près par l'appareil judiciaire. En quoi sacrifie-t-on la vie privée sur l'autel de pouvoirs accrus pour la police, alors qu'il s'agit d'un processus progressif faisant l'objet d'une supervision judiciaire? Comment votre association peut-elle formuler un tel commentaire?

M. Paisana : Je tiens à préciser ce que nous avons vraiment dit dans notre présentation. Notre présentation est exhaustive, et, de façon générale, nous appuyons le projet de loi. Nous avons formulé certaines recommandations précises au sujet des données de transmission et de ce dont vous avez parlé concernant les motifs raisonnables de soupçonner les motifs raisonnables de croire.

Vous constaterez aussi que nous acceptons et appuyons totalement l'infraction de cyberintimidation. Il est important pour moi que vous compreniez bien notre position.

En ce qui concerne la capacité des services de police d'enquêter et relativement à notre observation qui est liée aux deux domaines où, selon nous, il faudrait appliquer un seuil plus élevé, nous ne croyons pas que cela nuira à la gestion des types d'infractions dont nous parlons.

Vous avez tout à fait raison : le gouvernement devait réagir aux cas tragiques dont on a entendu parler, et il l'a fait. De façon générale, nous appuyons ce qui a été fait, mais réfléchissons concrètement à ce que ces cas nous révèlent : un plaignant dit à la police que quelqu'un partage une image intime de lui sans son consentement. À l'heure actuelle, aux termes du présent projet de loi, grâce à l'inclusion de la nouvelle infraction de cyberintimidation, on aura là des motifs raisonnables clairs de croire qu'une infraction a été commise. Il n'est pas nécessaire d'appliquer la norme du soupçon raisonnable. Un plaignant est là. Il peut identifier une image et il affirme qu'il n'a pas consenti à son partage. Cela respecte sans problème les critères liés au seuil plus élevé. Il ne s'agit pas d'un seuil insurmontable.

La différence, c'est lorsque la situation est telle qu'on ne bénéficie pas d'une preuve manifeste. Lorsqu'on n'a qu'un simple soupçon et qu'on respecte à peine le seuil du soupçon raisonnable. Lorsqu'il est question de renseignements de nature délicate

where someone has gone to a website, how often they've gone there, it can reveal a great deal about that person, and we suggest that in recognition of that, a higher standard should be employed vis-a-vis transmission data.

Senator McIntyre: Thank you, Mr. Paisana, for your presentation. I note that the Canadian Bar Association has made several recommendations. I'm not going to get into those, but I would like to touch on another topic.

In the *Spencer* decision, the court also noted that voluntary assistance could still be provided in exigent circumstances pursuant to reasonable law or where there's no reasonable expectation of privacy, contrary to the situation involving Mr. Spencer, thus making 487.0195 applicable, and as we know, that section will be replacing 487.014, which is the immunity section. So my question is this: Are you satisfied that the bill addresses the issue of exigent circumstances as raised in the *Spencer* decision?

Mr. Paisana: In my view, what *Spencer* clarifies is that where there are exigent circumstances, which they define as imminent harm, the police are able to request information outside of the scope of the legislation. That's my reading of what they have to say about that.

With respect to the immunity, the decision leaves untouched the concept that where there is no reasonable expectation of privacy then an individual cannot bring or does not have standing to bring a challenge to the admissibility of that evidence. That is literally the first step before anyone can make a challenge under section 8 of the Charter. They have to establish that they in fact have a reasonable expectation of privacy in the records that are sought to be admitted.

Senator McIntyre: That's right. In other words, common-law authority was not sufficient to constitute lawful authority, and therefore you need a warrant or a situation where you have exigent circumstances.

Mr. Paisana: Yes.

[*Translation*]

Senator Dagenais: In your brief, you say that you would prefer to see prevention and education initiatives for teenagers. No one can be against that.

However, do you not feel that, in addition to education and prevention, we still need a penalty in place as a deterrent?

comme l'historique de navigation, les sites consultés par une personne, la fréquence à laquelle elle les consulte, on peut en apprendre beaucoup ainsi au sujet d'une personne, et nous faisons valoir que, pour cette raison, on devrait utiliser une norme plus élevée en ce qui concerne les données de transmission.

Le sénateur McIntyre : Merci, monsieur Paisana, de votre exposé. Je souligne que l'Association du Barreau canadien a formulé plusieurs recommandations dont je ne parlerai pas parce que je veux vous parler d'autre chose.

Dans l'arrêt *Spencer*, la cour a aussi souligné qu'on pourrait tout de même fournir une aide volontaire dans des circonstances contraignantes, dans des cas où une loi qui n'a rien d'abusif le permet ou lorsqu'il n'y a pas d'attentes raisonnables en matière de protection de la vie privée, ce qui n'était pas le cas dans le dossier de M. Spencer, qui exigent l'application de l'article 487.0195, lequel, comme nous le savons, remplacera l'article 487.014, qui porte sur l'immunité. Ma question est la suivante : selon vous, le projet de loi règle-t-il la question des circonstances contraignantes soulevée par la cour dans l'arrêt *Spencer*?

M. Paisana : Selon moi, ce que l'arrêt *Spencer* précise, c'est que, lorsqu'il y a des circonstances contraignantes — ce que la cour définit comme étant un préjudice imminent —, les services de police peuvent demander des renseignements non visés par la loi. C'est ce que j'ai compris de sa position à ce sujet.

En ce qui concerne l'immunité, l'arrêt ne modifie en rien l'idée selon laquelle une personne ne peut pas contester l'admissibilité d'un élément de preuve et n'a pas le pouvoir de le faire lorsqu'elle n'a aucune attente raisonnable en matière de protection de la vie privée. Il s'agit littéralement du premier critère qu'une personne doit respecter avant de pouvoir contester quoi que ce soit aux termes de l'article 8 de la Charte. Elle doit premièrement établir qu'elle avait effectivement une attente raisonnable en matière de protection de la vie privée à l'égard des dossiers qu'on tente d'admettre en preuve.

Le sénateur McIntyre : C'est exact. En d'autres mots, la jurisprudence de common law n'était pas suffisante pour constituer une autorité légitime, et, par conséquent, il faut un mandat ou une situation où il y a des circonstances contraignantes.

M. Paisana : C'est exact.

[*Français*]

Le sénateur Dagenais : Dans votre mémoire, vous dites qu'il serait préférable de faire de la prévention, de la sensibilisation et de l'éducation auprès des adolescents. On ne peut pas être contre cela.

D'un autre côté, ne pensez-vous pas que, mis à part l'éducation et la prévention, en fin de compte, il faille une sanction qui aurait un effet dissuasif?

[*English*]

Mr. Paisana: Yes, and we don't take issue with the government's ability or right to criminalize youth in the appropriate circumstances. Our position is a nuanced one in that we recognize that in extreme situations there should be a criminal sanction. However, it is also a recognition in our submission that the criminal law should not be the answer to all of society's ills, particularly with respect to a complex issue such as youth cyberbullying.

Senator Batters: Thank you very much for being here today. I know the CBA testified before the House of Commons committee last spring. It wasn't you personally. It was one of your colleagues. Correct?

Mr. Paisana: Yes.

Senator Batters: I'm not sure if you've had an opportunity to read the testimony from the House of Commons committee hearings on the bill, but I note that the committee studied it for about 10 days, hearing from more than 40 witnesses, and there was extensive discussion about the investigative powers provision of the bill. I see that the first recommendation that the CBA has provided in its brief today is that it recommends dividing Bill C-13 into two distinct bills, as we've heard from some other legal witnesses. There's a split of opinion on that with other witnesses on this particular matter, but I'm not really sure what more could be added if a separate study was done again. That seems to be the contention of some, that we split it and study it again. Already we've had a number of witnesses come before both the House of Commons committee and the Senate committee. You might have heard Mr. Canning's comments. He said we need this bill and the police need these tools to prevent another tragedy such as the one that happened to his daughter, Rehtaeh Parsons.

We had Mr. Alan Hubley here before our committee recently, just before our constituency break week. He is the father of Jamie Hubley, who was cyberbullied here in Ottawa and unfortunately died by suicide. Mr. Hubley said:

> Bill C-13, in my view, is meant to help reduce cyberbullying and to help police obtain evidence needed to punish those among us who prey on our beautiful children. Our children need you to use your power as parliamentarians to protect them. Please ensure that change is progress by passing this bill and giving law enforcement the tools needed.

So I'm wondering if you could just comment on that and tell us whether you still believe that this bill needs to be delayed and split and studied another time.

[*Traduction*]

M. Paisana : Oui, et nous ne contestons pas la capacité ou le droit du gouvernement de criminaliser des jeunes lorsqu'il est approprié de le faire. Notre position est nuancée parce que nous reconnaissons que, dans certaines situations extrêmes, il faut imposer des sanctions pénales. Cependant, nous soulignons aussi dans notre présentation que le droit pénal n'est pas la réponse à tous les maux de la société, surtout pas à un enjeu aussi complexe que la cyberintimidation chez les jeunes.

La sénatrice Batters : Merci beaucoup d'être là aujourd'hui. Je sais qu'un représentant de l'ABC a témoigné devant un comité de la Chambre des communes au printemps dernier, mais ce n'était pas vous. C'était l'un de vos collègues, n'est-ce pas?

M. Paisana : Oui.

La sénatrice Batters : Je ne sais pas si vous avez eu l'occasion de lire le témoignage des audiences devant le comité de la Chambre des communes sur le projet de loi, mais je tiens à souligner que le comité s'est penché sur cette question pendant environ 10 jours, qu'il a entendu plus de 40 témoins, et qu'il y a eu une longue discussion sur la disposition touchant les pouvoirs d'enquête du projet de loi. Je constate que la première recommandation formulée aujourd'hui par l'ABC, dans son mémoire, est la division du projet de loi C-13 en deux projets de loi distincts, ce que d'autres témoins du milieu juridique nous ont aussi recommandé. Sur cet enjeu, les témoins sont partagés, mais je ne sais pas vraiment ce que donnerait une nouvelle étude distincte. Certains semblent tout de même proposer cette solution : séparer le projet de loi et l'étudier à nouveau. Le comité de la Chambre des communes et le comité du Sénat ont déjà rencontré un certain nombre de témoins. Vous avez peut-être entendu les commentaires de M. Canning. Il a dit que nous avons besoin de ce projet de loi et que les policiers ont besoin des outils prévus pour prévenir une autre tragédie comme celle dont a été victime sa fille, Rehtaeh Parsons.

Nous avons récemment accueilli M. Alan Hubley, juste avant la semaine de relâche durant laquelle nous retournons dans notre circonscription. Il est le père de Jamie Hubley, qui a été victime de cyberintimidation, ici même, à Ottawa, et qui s'est malheureusement enlevé la vie. Voici ce que M. Hubley avait à dire :

> À mon avis, le projet de loi C-13 vise à réduire la cyberintimidation et à aider la police à réunir les preuves permettant de punir ceux qui s'attaquent à nos magnifiques enfants. Nos enfants ont besoin que vous utilisiez votre pouvoir de parlementaire pour les protéger. [...] assurez-vous que le changement est synonyme de progrès en adoptant ce projet de loi et en donnant aux forces de l'ordre les outils nécessaires.

Je me demande si vous avez quelque chose à nous dire à ce sujet ou si vous croyez toujours qu'il faut retarder le processus, séparer le projet de loi et recommencer l'étude.

Mr. Paisana: There's no questioning the tragedy that has befallen some Canadians with respect to cyberbullying, and no one is suggesting that delay is appropriate. What we're suggesting is that appropriate attention be provided to the seriousness, that is, each aspect of this bill, and they're very different in the sense that one has to do with substantive criminal law and a substantive criminal offence and the other has to do with lawful access, and there are also provisions in the bill that seem far removed from either of those two things: for example, criminalizing the creation and sale of devices having to do with the stealing of TV signals and that type of thing.

It's always been our position that when dealing with complex issues such as lawful access and emerging issues such as the Internet, those should be reviewed and studied individually in order to have a more comprehensive understanding of the impact it may have going forward because, as the court has said in cases like *Tessling*, these laws are going to be applied into the future with forms of technology that we simply can't even foresee at this stage. Careful thought has to be given to each aspect of the legislation, but no one is suggesting that there should be delay. No one is suggesting that these individuals and Canadians don't deserve protection. In fact, the Canadian Bar Association strongly supports those aspects of the bill.

The Chair: A quick question or two on your concerns about the recklessness standard, removing it from the *mens rea*.

I gather that what you're talking about here is individuals who may fall under this who have no knowledge of the circumstances and no way to determine if the person depicted has consented. I gather what you're suggesting here is that these people should be free and clear if they distribute those kinds of images. It strikes me that if they bear no responsibility, it's going to greatly reduce the effectiveness of this section.

Shouldn't the courts be in a position to determine that the person who started the process will bear greater responsibility than someone down the line?

I'm concerned about the impact it would have on the effectiveness of the legislation if that was removed.

Mr. Paisana: I will make two points in response to that comment. The first is that the stated objective of this piece of legislation, as we understand it, is to combat cyberbullying, which has a very specific intent associated with it. We suggest that by having the recklessness standard, it's contributing to the capture of individuals who go beyond that stated objective. It captures individuals who lack that intent by virtue of the circumstances, and we have provided a factual example of how that could be.

M. Paisana : Personne ne minimise les tragédies dont ont été victimes certains Canadiens, en raison de la cyberintimidation, et personne non plus ne laisse entendre qu'il est approprié de retarder le processus. Nous disons seulement qu'il faut tenir compte du niveau de gravité de chaque aspect du projet de loi. En effet, ils sont très différents les uns des autres, parce que l'un concerne les règles de fond du droit pénal et d'une infraction criminelle, et l'autre porte sur l'accès légitime. En outre, il y a aussi des dispositions dans le projet de loi qui ne semblent aucunement liées à deux thèmes, comme la criminalisation de la création et de la vente de dispositifs associés au vol de signal de télévision et d'autres choses du genre.

Nous avons toujours affirmé que, lorsque nous traitons d'enjeux complexes, comme l'accès légal, et les nouveaux enjeux, comme ceux liés à Internet, il est préférable de procéder à un examen et à une étude distincts afin de pouvoir très bien comprendre leur impact, parce que la cour a dit dans des arrêts comme *Tessling* que les lois promulguées seront appliquées à l'avenir dans le cas de formes de technologies que nous ne pouvons tout simplement même pas concevoir actuellement. Il faut bien réfléchir à chaque aspect du projet de loi, mais, bien sûr, personne ne laisse entendre qu'il doit y avoir des retards. Personne ne laisse croire non plus que ces personnes et les Canadiens ne doivent pas être protégés. En fait, l'Association du Barreau canadien appuie fortement ces aspects du projet de loi.

Le président : J'ai une ou deux questions rapides pour vous au sujet de la norme d'insouciance et de son retrait de l'intention coupable.

Je crois comprendre que vous parlez des personnes qui pourraient être visées par la disposition sans pour autant avoir conscience des circonstances ni de la façon de déterminer si la personne représentée a donné son consentement. Si je vous comprends bien, vous suggérez que ces personnes devraient être jugées blanches comme neige si elles distribuent ce genre d'images. Selon moi, leur enlever toute responsabilité réduira grandement l'efficacité de l'article.

Les tribunaux ne devraient-ils pas pouvoir décider que la personne à l'origine du partage devrait assumer une plus grande responsabilité que ceux qui ont partagé le contenu par la suite?

Je suis préoccupé par l'impact que ce retrait pourrait avoir sur l'efficacité du projet de loi.

M. Paisana : J'ai deux choses à dire en réponse à ce que vous venez de dire. Premièrement, l'objectif explicite du projet de loi, tel que nous l'avons compris, est de lutter contre la cyberintimidation, comportement qui est associé à une intention bien précise. Nous sommes d'avis que, en adoptant la norme d'insouciance, on englobe des personnes qui n'étaient pas visées par l'objectif initial. On vise des personnes qui, compte tenu des circonstances, n'avaient pas l'intention en question, et nous avons fourni un exemple concret de la façon dont cela pourrait se produire.

The second point I would make about that is that the criminal law is not the sole answer. There are privacy statutes across provinces that deal with situations where someone has violated someone's reasonable expectation of privacy. I know in British Columbia we have a statute of that kind. There are civil remedies. There can be municipal laws. There are other responses short of what many consider to be the blunt tool that is the criminal law. That carries significant impacts.

The Chair: I guess the concern is that the distribution of images escalates when someone new gets it, passes it on to who knows how many people. What you're suggesting would, in my view, weaken the ability to deal with that situation.

Senator Baker: Thank you for your presentation and for the excellent work that you do in the law in British Columbia. We all appreciate it.

Let me ask you this question: You've litigated matters involving transportation of drugs and so on. You've presented a very good argument to the court as to the required standard of reasonable suspicion for an investigative detention, if you recall the truck case that you did such an excellent job on.

Here's my question: In *Spencer*, the Supreme Court of Canada compared this particular matter to that of a search conducted by a dog sniff, paragraph 47 of *Spencer*. Similarity, because a dog sniff is a search, according to Brown.

In order to justify that search of your luggage, your car or anything where you need a dog sniff — and the dog is never wrong, I don't think — you need reasonable suspicion. That's the standard. But you are saying here, and a lot of other witnesses are saying — and I don't disagree with you; I'm just looking for an answer to this question — why is a reasonable suspicion not sufficient in this legislation when it's sufficient in other searches that are conducted in our society under the Criminal Code and established case law? You quoted the case in 2013, Supreme Court of Canada, concerning a reasonable suspicion as it relates to the dog sniff. Why, then, do you say now that this is not justified under this legislation, when *Spencer* allowed the results of the search? Constitutional rights were violated, but the evidence went in. Why? The Supreme Court of Canada said because this is important to our society. Our society wants justice here.

So why do you draw that line so firmly as you've drawn it as it relates to the subject matter of this bill?

Deuxièmement, j'aimerais rappeler que le droit pénal n'est pas l'unique réponse possible. Il y a des lois provinciales qui traitent de situations où quelqu'un a violé l'attente raisonnable en matière de protection de la vie privée d'une autre. Je sais que la Colombie-Britannique possède ce genre de lois. Il y a des recours civils et des règlements municipaux. Il y a d'autres solutions à part le droit criminel, que beaucoup considèrent comme un outil grossier. Tout cela peut avoir d'importantes répercussions.

Le président : J'imagine que la préoccupation, c'est que la distribution des images s'aggrave lorsqu'une nouvelle personne les obtient et les redistribue à je ne sais combien d'autres personnes. Selon moi, votre suggestion minerait notre capacité de gérer de telles situations.

Le sénateur Baker : Merci de votre exposé et de l'excellent travail que vous faites dans le milieu juridique de la Colombie-Britannique. Nous l'apprécions tous.

Permettez-moi de vous poser la question suivante : vous avez plaidé des affaires liées au transport de drogues et ce genre de choses. Vous avez présenté un très bon argument à un tribunal quant à la norme des soupçons raisonnables requis pour détenir des gens aux fins d'enquête. Je parle, si vous vous en souvenez, du dossier du camion dans le cadre duquel vous aviez vraiment fait du bon travail.

Voici donc ma question : au paragraphe 47 de l'arrêt *Spencer*, la Cour suprême du Canada a comparé cette situation précise à celle d'une fouille réalisée par un chien renifleur. La similitude tient au fait que l'utilisation d'un chien renifleur est aussi assimilable à une fouille, selon l'arrêt *Brown*.

Afin de justifier la fouille d'un bagage, d'un véhicule ou de quoi que ce soit d'autre à l'aide d'un chien renifleur — et les chiens ne se trompent jamais, si je ne m'abuse —, il faut avoir un soupçon raisonnable. C'est la norme. Mais, ici, vous nous dites, comme beaucoup d'autres témoins... Je ne suis pas en désaccord avec vous, je veux simplement que vous répondiez à la question suivante : pourquoi un soupçon raisonnable n'est-il pas suffisant dans le projet de loi alors qu'il l'est pour d'autres fouilles réalisées dans notre société aux termes du Code criminel et de la jurisprudence établie? Vous avez cité un arrêt de la Cour suprême du Canada de 2013 qui portait sur la question du soupçon raisonnable et du recours à un chien renifleur. Pourquoi, alors, dites-vous maintenant que cette norme n'est pas justifiée aux termes du projet de loi, alors que, dans l'arrêt *Spencer,* la cour a admis les résultats de la fouille? Des droits constitutionnels ont été violés, mais les éléments de preuve ont été acceptés. Pourquoi? La Cour suprême du Canada a dit que c'était parce que c'était important pour notre société. Notre société demande justice ici.

Alors pourquoi faites-vous une distinction aussi claire en ce qui concerne le contenu du présent projet de loi?

Mr. Paisana: The answer lies in the subject matter of transmission data. To be clear, we're not taking issue with the reasonable suspicion aspect of this bill and other sections. For example, we agree that reasonable grounds to suspect are appropriate for the preservation demand.

What we're saying is that when you get to transmission data, because of the nature of that data, which is that the data can reveal a great deal about someone — and who knows in the future how much more it can reveal with the advances of technology — a higher standard should be required, because it reveals more about the person. That's what *Spencer* talks about, that subscriber information is just a name. It's just an address, just a telephone number. But that's not all it is. It provides the key; it provides the link to this Internet history that provides intimate details of Mr. Spencer's life.

That's why it was such a serious violation, in their view. Why it was considered a significant privacy interest is because it reveals a great deal about that individual, as opposed to the smell surrounding a piece of luggage, which you can see distinctively reveals a lot less about an individual.

Senator Baker: It's still a search.

Mr. Paisana: It's still a search, but it's a search that can be conducted at a lower level because it recognizes that there's a different privacy interest at stake, and that's what *Chehil* and *Spencer* talked about: What is the nature of the privacy interest? It's something to say that the air surrounding a piece of luggage is one thing, but revealing someone's Internet history and linking it to a particular individual is a whole different story, in our view.

Senator Baker: *Spencer* came in after the House of Commons had their hearings. It was right after, because they finished their hearings on June 12, and your association gave evidence in the early part of June, and on June 14, the Supreme Court of Canada made the decision in *Spencer*. I guess what you're saying is the picture has changed because of *Spencer*. Thank you.

Senator McInnis: Just on that point: One of the questions we always have here is balancing privacy with the protection of Canadians and safety of Canadians. It seems to me, after doing a fair bit of research on this, the word "trust" comes to the fore. It's very important. When we had the law enforcement people here, they said that any information they get will be strictly controlled and limited to law enforcement officials, fully trained in the procedures and subject to auditing and reporting oversight.

M. Paisana : La réponse réside dans la nature des données de transmission. Soyons clairs, nous ne contestons pas le recours à la norme du soupçon raisonnable dans le projet de loi et dans d'autres articles. Par exemple, nous reconnaissons que la norme des motifs raisonnables de soupçonner est appropriée dans le cas des demandes de préservation.

Ce que nous disons, c'est que, lorsqu'il est question des données de transmission, en raison de la nature de ces données, qui peuvent en dire beaucoup au sujet d'une personne — et qui sait à quel point nous pourrons en apprendre au sujet d'une personne grâce à ces données à l'avenir en raison des percées technologiques —, il faudrait imposer une norme plus élevée, parce que ces renseignements en disent long sur les gens. Dans l'arrêt *Spencer*, la cour parle des renseignements relatifs aux abonnés : il ne s'agit pas que d'un nom, d'une adresse et d'un numéro de téléphone, c'est plus que ça. Ces renseignements sont la clé qui donne accès à l'historique de navigation, qui lui, fournit des détails intimes sur la vie de M. Spencer.

C'est pour cette raison que, selon la cour, il s'agissait d'une atteinte grave. La cour a considéré que cela mettait en jeu un droit en matière de vie privée beaucoup plus important parce que l'information révélait beaucoup de choses au sujet de cette personne, contrairement à l'odeur d'une valise, qui, vous comprenez bien, en dit beaucoup moins au sujet d'une personne.

Le sénateur Baker : C'est tout de même une fouille.

M. Paisana : C'est tout de même une fouille, mais il s'agit d'une fouille qui peut être réalisée à un niveau inférieur parce qu'on reconnaît qu'elle met en jeu un droit en matière de vie privée différent, et c'est ce dont la cour a parlé dans les arrêts *Chehil* et *Spencer :* quelle est la nature du droit en matière de vie privée? C'est une chose de dire que l'air près d'une valise a telle ou telle caractéristique, mais révéler l'historique de navigation sur Internet d'une personne et l'associer à une personne précise est une tout autre histoire, selon nous.

Le sénateur Baker : L'arrêt *Spencer* a été rendu après les audiences de la Chambre des communes. C'était tout juste après, parce que les audiences se sont terminées le 12 juin, et que votre association a témoigné au début de juin. La Cour suprême du Canada a rendu sa décision dans l'arrêt *Spencer* le 14 juin. J'imagine que vous dites que la situation a changé en raison de l'arrêt *Spencer*. Merci.

Le sénateur McInnis : J'aimerais dire une chose : un des enjeux dont nous devons toujours tenir compte, ici, c'est de trouver le juste équilibre entre la vie privée et la protection et la sécurité des Canadiens. J'ai l'impression, après avoir fait pas mal de recherche à ce sujet, que le mot « confiance » est à l'avant-plan. C'est très important. Lorsque nous avons accueilli des représentants de la loi, ils ont dit que tous les renseignements qu'ils obtiennent font l'objet d'un contrôle strict et seront uniquement consultés par des représentants de l'application de la loi qui ont reçu toute la formation nécessaire sur les procédures et dont le comportement ferait l'objet de vérifications et de rapports.

It seems to me that parliamentarians — and we here in the Senate now — in considering this have to weigh that we have great concerns about what's taking place, and youth committing suicide, horrific, and yet we too are interested in privacy. All you have to do is look at anything from the Charter of Rights to the Privacy Act to the Federal Accountability Act. All kinds of acts have been put in law in this country. Where is the problem?

I'm not questioning whether your association trusts the law enforcement. I know you do. But it strikes me that when we're making decisions like that we have to come down as fairly as we can in giving the law enforcement officers the tools to effectively protect Canadians.

Mr. Paisana: No one is taking issue with the government's ability to provide police officers with the tools necessary to investigate crime, but when we make suggestions like "just trust the police," it provides a slippery slope that we have to guard against at all times.

As lawyers and legislators, we have to guard against falling into the habit of simply relying on the police to do the right thing. We trust that they will do the right thing most of the time. But that's why we need judicial oversight. This is a democracy that relies on that aspect of the judicial system to ensure that section 8 is observed to the greatest extent possible while still providing for the investigation of crime.

Senator McInnis: With respect, I'm not questioning whether your association or anyone trusts the police. I think we all do. Canadians admire the police. I guess what we're saying is that we're being asked to protect Canadians, and we're using the very best tools that we possibly can, and that's exactly what this bill does.

In my career, I've seen legislation that could go through in three to six months. This bill has been in the making for years, and I think Canadians want us to act, not with reckless abandon but with sincerity and effectiveness and efficiencies, but guarding privacy as well.

Mr. Paisana: What I think is that Canadians expect that balance to be struck appropriately. As we've seen with previous incarnations of this bill, which we've always had opportunity, thankfully, to comment upon, we've taken issue with previous incarnations that went too far, in our respectful view. We say those changes are appropriate.

That's why the recommendations we say in this round of study are much more moderate than the ones we have suggested in the past because, frankly, the government did the right thing and listened to many of the witnesses who came forward and

Selon moi, les parlementaires — et nous sommes actuellement au Sénat — qui se penchent sur cette question doivent tenir compte du fait que nous sommes extrêmement préoccupés par ce qui se passe, les jeunes qui se suicident, ces histoires horribles, et, malgré tout, nous aussi voulons protéger la vie privée. Vous n'avez qu'à regarder tout ce qui a été fait, de la Charte des droits à la Loi sur la protection des renseignements personnels en passant par la Loi fédérale sur la responsabilité. Tous ces types de lois ont été mis en place au pays. Quel est le problème?

Je ne vous demande pas si votre association fait confiance aux organismes d'application de la loi. Je sais que vous leur faites confiance. Mais il semble évident pour moi que, lorsque nous prenons des décisions comme celle-ci, il faut le faire de la façon la plus équitable en donnant aux représentants de l'application de la loi les outils dont ils ont besoin pour bien protéger les Canadiens.

M. Paisana : Personne n'en veut à la capacité du gouvernement de fournir aux agents de police les outils dont ils ont besoin pour enquêter lorsqu'il y a des crimes, mais lorsque nous disons des choses comme : « Faites simplement confiance à la police », c'est une pente glissante contre laquelle nous devons toujours nous protéger.

En tant qu'avocats et législateurs, nous devons faire attention de ne pas prendre l'habitude de tout simplement nous fier à la police pour qu'elle fasse bien les choses. Nous savons qu'elle fera la bonne chose la plupart du temps. Mais c'est la raison pour laquelle nous avons besoin d'une surveillance judiciaire. Nous sommes dans une démocratie qui s'appuie sur cet aspect du système judiciaire pour s'assurer qu'on respecte le plus possible l'article 8 tout en permettant la tenue d'enquête sur les crimes.

Le sénateur McInnis : Avec tout le respect que je vous dois, je ne me demande pas si votre association ou quiconque fait confiance à la police. Je crois que nous lui faisons tous confiance. Les Canadiens admirent les forces de l'ordre. Ce que nous disons, j'imagine, c'est qu'on nous demande de protéger les Canadiens, et nous utilisons les meilleurs outils que nous pouvons, et c'est exactement ce que l'on fait avec ce projet de loi.

Dans ma carrière, j'ai vu des projets de loi entrer en vigueur en trois à six mois. Ce projet de loi est en cours d'élaboration depuis des années, et je crois que les Canadiens veulent que nous passions à l'action, pas de façon téméraire, mais avec sincérité, efficacité et efficience, et tout en assurant la protection des renseignements personnels.

M. Paisana : D'après moi, les Canadiens veulent que nous trouvions le juste équilibre et que nous le fassions de façon appropriée. Comme nous l'avons vu dans les versions précédentes du projet de loi, que nous avons toujours eu l'occasion de commenter, ce dont nous sommes reconnaissants... Nous avons contesté les versions précédentes qui, selon nous, allaient trop loi. Nous affirmons que ces changements sont appropriés.

C'est la raison pour laquelle les recommandations que nous formulons cette fois-ci sont beaucoup plus modérées que celles que nous avions formulées dans le passé parce que, franchement, le gouvernement a fait la bonne chose et a écouté bon nombre des

presented concerns about the overreaching aspects of parts of the previous incarnations. We are simply asking for similar consideration vis-à-vis very narrow aspects of this most recent incarnation. As you can see from our 25-page submission, we don't take issue with most of what is included in this bill.

Senator McIntyre: I'm looking at recommendation number 3, and I notice that you're calling for the amendment of section 162.1, which says:

> No person shall be convicted of an offence under this section if the distribution, transmission, selling, making available or advertising that forms the subject-matter of the charge is for the public's information or is a matter of public interest.

I was just wondering what you meant by "matter of public interest," because, as you know, Bill C-13 includes a defence of public good. That defence is well established in Canadian law, as included in a few of the sections in the Criminal Code, including voyeurism and obscenity offences. Could you comment on that, please?

Mr. Paisana: Yes. That aspect of the bill was advocated for by our privacy and access to information law section. What I understand the recommendation to refer to is simply a refinement of the public good defence in order to make explicit that it's with respect to information that is for the public information and public interest. They're not necessarily at odds. I think it's more a refinement of the language as opposed to failing to recognize that there is a defence built in.

We concede that it may be that the public interest and public information aspects that we're recommending could, in fact, be built into the public good vis-à-vis interpretation of that defence in the courts.

The Chair: Thank you again, sir, for your appearance, your testimony and the good work the CBA has done with respect to its consideration of the legislation. We very much appreciate it.

For our next panel, from the Office of the Privacy Commissioner of Canada, we have Daniel Therrien, who is the Privacy Commissioner; Patricia Kosseim, Senior General Counsel and Director General; and Daniel Caron, Legal Counsel.

Mr. Therrien, welcome along with your staff. I understand you have an opening statement, sir. Please proceed.

témoins qui sont venus lui formuler leurs préoccupations au sujet des domaines où les versions précédentes allaient trop loin. Nous vous demandons simplement de tenir compte de façon semblable de nos recommandations relativement à des aspects très pointus de la plus récente version. Comme vous pouvez le voir dans notre mémoire de 25 pages, nous n'avons aucun problème avec la majeure partie du projet de loi.

Le sénateur McIntyre : J'examine la recommandation nº 3 et je constate que vous demandez la modification de l'article 162.1 qui porte que :

> Nul ne peut être déclaré coupable d'une infraction en vertu du présent article si la distribution, la transmission, la vente, le fait de rendre accessible ou la publicité qui constitue l'objet de l'accusation est destiné à l'information du public ou constitue une question d'intérêt public.

Je me demande ce que vous voulez dire par « une question d'intérêt public », parce que, comme vous le savez, le projet de loi C-13 prévoit un moyen de défense lié au bien public. Ce moyen de défense est bien établi dans le droit canadien, et il figure dans certains articles du Code criminel, y compris ceux sur le voyeurisme et les infractions liées à l'obscénité. Pouvez-vous nous parler de cet aspect?

M. Paisana : Oui. Cet aspect du projet de loi a été demandé par notre Section nationale du droit à la vie privée et de l'accès à l'information. Si j'ai bien compris, la recommandation visait simplement une amélioration du moyen de défense lié au bien public afin de dire explicitement qu'on parle de renseignement qui est destiné à l'information du public ou qui constitue une question d'intérêt public. Je ne crois pas qu'il y a là de contradictions. Je crois que si on tente davantage d'améliorer le libellé, ce n'est pas que nous n'avons pas reconnu qu'une telle défense était déjà prévue.

Nous reconnaissons qu'il est possible que des aspects liés à l'intérêt public ou à l'information du public que nous recommandons pourraient, en fait, être inclus dans la défense du bien public en ce qui concerne l'interprétation de ce moyen de défense par les tribunaux.

Le président : Encore merci, monsieur, de votre participation, de votre témoignage et du bon travail qu'a fait l'ABC dans son évaluation du projet de loi. Nous l'apprécions beaucoup.

Nous passons à notre prochain groupe de témoins. Nous accueillons Daniel Therrien, commissaire à la protection de la vie privée du Canada; Patricia Kosseim, avocate générale principale et directrice générale; et Daniel Caron, conseiller juridique, du Commissariat à la protection de la vie privée du Canada.

Monsieur Therrien, bienvenue, et bienvenue à votre personnel. Je crois savoir que vous avez une déclaration préliminaire, monsieur. La parole est à vous.

[*Translation*]

Daniel Therrien, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada: Thank you, honourable senators, for the invitation to comment on Bill C-13, the Protecting Canadians from Online Crime Act.

My office has provided this committee with a written submission in which we support the creation of new criminal offences aimed at combating cyberbullying, but identify significant privacy risks associated with the surveillance powers being proposed.

Let me highlight a few of our key points today. On the issue of thresholds, I recommend that the reasonable grounds to believe standard prevail as the appropriate judicial threshold for authorization of the new production orders and warrants. Courts have upheld the lower reasonable suspicion standard only in limited situations where privacy interests are reduced or where state objectives of public importance are predominant.

The government defends the reasonable suspicion thresholds in Bill C-13 partly based on the argument that the information sought is not very sensitive and triggers a lower expectation of privacy. With respect, I disagree.

As the Supreme Court of Canada recently reminded us in the *Spencer* decision, protecting privacy interests requires us to look not only at the specific information being sought — no matter how seemingly innocuous — but also at what the information may further reveal about the activities of an individual.

A paper recently published by our office, entitled *Metadata and Privacy*, demonstrates how various forms of transactional and transmission data can indeed reveal very sensitive details about an individual.

The government further justifies the reasonable suspicion threshold on the grounds that combatting cyberbullying or online child exploitation are important state objectives, which of course they are.

However, it is important to remember that these new investigative tools would sweep up vast amounts of personal information by an open-ended group of public officers for a wide range of much less compelling purposes than the fight against cyberbullying.

[*English*]

As the Supreme Court said in *Spencer*, privacy interests do not depend on whether privacy shelters legal or illegal activity, or on the legal or illegal nature of the information being sought. The issue is therefore not one of concealing illegal use of the Internet

[*Français*]

Daniel Therrien, commissaire à la protection de la vie privée du Canada, Commissariat à la protection de la vie privée du Canada : Je vous remercie, honorables sénateurs, de nous avoir invités à nous prononcer sur le projet de loi C-13, la Loi sur la protection des Canadiens contre la cybercriminalité.

Le commissariat a fourni au comité un mémoire dans lequel nous appuyons la création de nouvelles infractions criminelles pour combattre la cyberintimidation, tout en soulignant les risques importants relatifs à la protection de la vie privée que posent les pouvoirs de surveillance proposés.

J'aimerais maintenant signaler nos principaux points. En ce qui concerne la question des seuils de preuve, je recommande que la norme liée aux motifs raisonnables de croire s'applique à l'autorisation de nouvelles ordonnances de communication et de nouveaux mandats. Les tribunaux ont approuvé la norme inférieure du soupçon raisonnable uniquement dans certaines situations où les intérêts en matière de protection de la vie privée sont réduits ou lorsque les objectifs d'ordre public de l'État sont prédominants.

Le gouvernement défend le seuil du soupçon raisonnable en partie sur la foi de l'argument voulant que l'information recherchée ne soit pas de nature très sensible et qu'elle entraîne donc des attentes réduites en matière de vie privée. En toute déférence, je ne suis pas de cet avis.

Comme la Cour suprême du Canada nous l'a récemment rappelé dans l'affaire *Spencer*, la protection des intérêts relatifs à la vie privée exige non seulement que nous examinions l'information recherchée, même si elle peut paraître inoffensive, mais aussi ce que l'information peut révéler quant aux activités d'un individu.

Un document publié récemment par le commissariat, intitulé *Métadonnées et vie privée*, démontre de quelle façon les différentes formes de données relatives à des transactions et à des communications peuvent, en fait, révéler des renseignements très sensibles au sujet d'une personne.

Le gouvernement justifie, en outre, le seuil du soupçon raisonnable par le fait que la lutte à la cyberintimidation ou à l'exploitation en ligne des enfants est un objectif d'ordre public important. Elle l'est, bien entendu.

En revanche, il importe de rappeler que ces nouveaux outils d'enquête permettraient à un groupe indéfini de fonctionnaires publics de rassembler une immense quantité de renseignements personnels à plusieurs fins beaucoup moins importantes que la lutte à la cyberintimidation.

[*Traduction*]

Comme l'a affirmé la Cour suprême dans *Spencer*, les intérêts en matière de vie privée ne dépendent pas de la question de savoir si le droit à la vie privée masque une activité illégale ou non, ou de la nature légale ou illégale de l'information recherchée. La

for cyberbullying or child pornography but of protecting the privacy interests that people generally have with respect to home computers they use for private purposes.

While some may argue that this reasoning could create a virtual space where crime can flourish, the court rejected that argument in *Spencer*, noting that investigators had ample evidence to obtain a production order for the information they were seeking.

Should the committee support the lower standard of reasonable suspicion, we suggest adding language that would limit the use of information obtained through these powers to the investigation of the alleged crime specified in the court application.

With regard to section 487.095, this immunity provision would protect from legal liability those who voluntarily disclose personal information in response to government requests without a warrant.

Where the state seeks access to personal information held by organizations, including Internet service providers, *R. v. Spencer* clearly limits warrantless searches to situations where there are exigent circumstances, a reasonable law, or where the information does not attract a reasonable expectation of privacy. Carrying out a "reasonable expectation of privacy" analysis is complex and highly contextual, but how are organizations and individuals expected to do this in a given case?

Several months after *Spencer*, Canadians are still in the dark about what may happen to their personal information. There appears to be wide variation in how the *Spencer* decision is being interpreted. I would therefore urge Parliament to put an end to this state of ambiguity and clarify what, if anything, should remain of the common-law policing powers to obtain information without a warrant post-*Spencer*.

Finally, on the need for transparency and accountability, the Supreme Court of Canada has in the past invited Parliament to decide what accountability and oversight mechanisms would be appropriate to ensure the reasonableness of a law, while recognizing the practical and policy implications. I would therefore ask parliamentarians to build into Bill C-13 the necessary reporting mechanisms that would allow Canadians to hold government to account for the use of these significant new powers as well as requests without a warrant.

question concerne non pas la dissimulation de l'usage illicite d'Internet pour la cyberintimidation ou la pornographie infantile, mais bien la protection des intérêts en matière de vie privée des gens, de manière générale, relativement aux ordinateurs qu'ils utilisent dans leur domicile à des fins privées.

Alors que certains considèrent que ce raisonnement pourrait créer un espace virtuel où le crime peut foisonner, la cour a rejeté cet argument dans l'arrêt *Spencer* en signalant que les enquêteurs disposaient de renseignements détaillés permettant d'obtenir une ordonnance de communication visant les renseignements recherchés.

Si le comité donne son aval à la norme moins élevée du soupçon raisonnable, nous suggérons d'ajouter une modification pour faire en sorte que l'utilisation de l'information obtenue par l'exercice de ces pouvoirs soit limitée à l'enquête de l'infraction précisée dans la demande au tribunal.

En ce qui a trait à l'article 487.095, cette disposition sur l'immunité protégerait contre toute responsabilité légale toute personne qui divulgue volontairement des renseignements personnels en réponse à des demandes du gouvernement sans mandat.

Là où l'État cherche à accéder à des renseignements personnels détenus par des organisations, y compris les fournisseurs de services Internet, *R. c. Spencer* limite clairement les perquisitions sans mandat aux situations où il y a des circonstances contraignantes, une loi qui n'a rien d'abusif, ou où l'information ne fait pas l'objet d'une attente raisonnable en matière de vie privée. L'exécution d'une analyse de l'« attente raisonnable en matière de vie privée » est complexe et dépend fortement du contexte. Comment peut-on s'attendre à ce que les organisations et les particuliers fassent cette analyse dans une situation donnée?

Plusieurs mois après *Spencer*, les Canadiens ne savent toujours pas ce qui pourrait advenir de leurs renseignements personnels. Il semble y avoir de grandes variations dans la manière d'interpréter la décision *Spencer* et d'y réagir. J'encourage vivement le Parlement à mettre fin à cette situation ambiguë et à clarifier quels sont les pouvoirs de la police en common law, le cas échéant, pour obtenir de l'information sans mandat suite à l'arrêt *Spencer*.

Enfin, sur la question de la transparence et de l'imputabilité, la Cour suprême du Canada a invité par le passé le Parlement à déterminer quels mécanismes de surveillance et d'imputabilité il conviendrait de mettre en place pour assurer le caractère raisonnable d'une loi tout en reconnaissant les implications d'ordre pratique et politique. Je demande donc aux parlementaires, pendant qu'ils en ont encore l'occasion, d'enchâsser dans le projet de loi C-13 les mécanismes d'imputabilité permettant aux Canadiens de tenir le gouvernement responsable de l'exercice de ces nouveaux pouvoirs importants et lorsqu'il effectue des demandes sans mandat.

Thank you very much for the opportunity to comment on this important bill, and I welcome your questions.

The Chair: Thank you.

Senator Baker: Thank you to the Privacy Commissioner and his staff.

The Privacy Commissioner of Canada was, of course, one of the quoted interveners in the *Spencer* case, and I see you have with you two of the people who appeared before the Supreme Court of Canada concerning this matter.

Commissioner, *Spencer* was about your act, the PIPEDA. It wasn't about a warrant or a production order; it was about section 7 of the PIPEDA. And a resolution that, according to the Supreme Court of Canada, revolved around the definition of "lawful authority" in that section.

My first question to you is this: What direction would you give? You have to adjudicate matters that arise under this act. Under the act, the way it's worded, a police officer doesn't need anything, not reasonable grounds to suspect or anything, just a letter to the service provider, if they're covered by PIPEDA, and the information would be given if they had lawful authority to do so.

What is your opinion now on your PIPEDA? *Spencer* came after your appearance before the House of Commons committee, so this is a new area, and you've changed your submission substantially to what you said before the house. You're asking for definitive action here on the part of the government.

What do you have to say now about PIPEDA, the act that you administer?

Mr. Therrien: Thank you for the question. This is not an easy question to answer, so let me take a bit of time to explain.

PIPEDA is certainly relevant to this issue in that there's a provision in it which authorizes, by exception to the general rule, that private organizations should keep confidential the information they have with respect to individuals.

In section 7, PIPEDA authorizes the disclosure by private organizations to government of information sought by government and that private organizations voluntarily disclose on the basis of the letters you were referring to. So that's what PIPEDA does.

Je vous remercie de m'avoir donné l'occasion de vous parler de ce projet de loi important. Je serai maintenant heureux de répondre à vos questions.

Le président : Merci.

Le sénateur Baker : Je remercie le commissaire à la protection de la vie privée et son personnel.

Le commissaire à la protection de la vie privée du Canada était, bien sûr, l'un des intervenants cités dans le cadre de l'affaire *Spencer*, et je constate que vous êtes accompagné de deux personnes qui ont témoigné devant la Cour suprême du Canada à ce sujet.

Monsieur le commissaire, *Spencer* concernait votre loi, la LPRPDE. Cette affaire ne concernait pas un mandat ou une ordonnance de communication; elle concernait l'article 7 de la LPRPDE et une résolution qui, selon la Cour suprême du Canada, tournait autour de la définition que donne cet article à « autorité légitime ».

Voici ma première question : quelle directive donneriez-vous? Vous devez vous prononcer sur des enjeux soulevés par cette loi. Selon la loi, la façon dont elle est écrite, un policier n'a besoin de rien, pas de motifs valables ni quoi que ce soit, il n'a qu'à envoyer une lettre au fournisseur de services, s'il est visé par la LPRPDE, et l'information lui serait donnée s'il a l'autorité légitime de la demander.

Actuellement, que pensez-vous de la LPRPDE? L'arrêt *Spencer* est survenu après votre témoignage devant le comité de la Chambre des communes, donc, il s'agit d'un nouveau domaine, et votre discours a passablement changé depuis votre passage à la Chambre. Vous demandez ici au gouvernement de prendre des mesures concrètes.

Qu'avez-vous maintenant à dire à propos de la LPRPDE, la loi dont vous veillez à l'application?

M. Therrien : Merci pour votre question. Ce n'est pas une question à laquelle il est facile de répondre, donc laissez-moi le temps de vous fournir quelques explications.

La LPRPDE est sans aucun doute liée à l'enjeu en cause, puisqu'elle renferme une disposition qui autorise la divulgation de renseignements, ce qui constitue une exception à la règle générale selon laquelle les organisations privées doivent garder confidentiels les renseignements qu'elles possèdent sur les personnes.

L'article 7 de la LPRPDE autorise les organisations privées à divulguer sur demande des renseignements au gouvernement et à les divulguer de façon volontaire lorsqu'elles reçoivent les lettres dont vous avez parlé. C'est de cette façon que la LPRPDE agit.

The Supreme Court has clearly significantly limited the extent to which these letters can actually result in the disclosure of information by private organizations to law enforcement agencies where there is a reasonable expectation of privacy. That's an important notion, "reasonable expectation of privacy."

Where there is a reasonable expectation of privacy, and the court judgment is very useful in giving guidance on what that term means with respect to information on the Internet, the court clarified that personal information that may sound innocuous or banal but that may reveal the activities of an individual on the Internet is sensitive and subject to a reasonable expectation of privacy.

When there is a reasonable expectation of privacy, the court adds that disclosure can occur only in one of three circumstances: where there is a judicial authorization, where there are exigent circumstances, or where there is a reasonable law. So the common law ceases to be a lawful authority for the purposes of PIPEDA.

So far, I've explained how *Spencer* significantly limits the disclosure of information by private organizations to government, but all of this depends on whether there is a reasonable expectation of privacy. The court says nothing about limitations when there is no reasonable expectation of privacy.

The reason I'm calling for clarity on this question is that we're hearing from various important players in this debate. Minister MacKay has said that the bill does not need to be changed as a result of *Spencer*, which leads one to wonder what impact in practice *Spencer* will have.

Many departments that were asked by certain members of Parliament to explain when they receive information from private organizations have revealed no information at all, so we don't know what they are obtaining. Some telecommunication companies have said, post-*Spencer*, that they will no longer provide information to government except in the three circumstances I've described, and others have said nothing.

So I'm left, certainly, and I think Canadians are left, with a judgment that is very useful, which limits disclosure by private organizations to government when there is a reasonable expectation of privacy, which leaves a lot of room for interpretation by various players on when there is or is not a reasonable expectation of privacy.

Senator McInnis: Thank you very much. This is not my question, but what we were told by law enforcement is that basically *Spencer* has shot them down; they're not giving anything. But that's not solace, necessarily.

La Cour suprême a limité de façon importante la divulgation des renseignements à des organisations d'application de la loi par des organisations privées à la suite de la réception de ces lettres lorsqu'il existe une attente raisonnable en matière de vie privée. L'attente raisonnable en matière de vie privée constitue une notion importante.

Lorsqu'il existe une attente raisonnable en matière de vie privée, et le jugement du tribunal explique bien ce que ce terme signifie au chapitre des renseignements sur Internet, le tribunal a conclu que les renseignements personnels qui pouvaient sembler inoffensifs ou banals, mais qui sont susceptibles de révéler les activités d'une personne sur Internet, constituent des informations délicates et sont protégés par une attente raisonnable en matière de vie privée.

Lorsqu'il y a une attente raisonnable en matière de vie privée, le tribunal ajoute que la divulgation peut se faire seulement dans l'une de trois circonstances : lorsqu'il y a une autorisation judiciaire préalable, des circonstances contraignantes ou une loi qui n'a rien d'abusif. La common law cesse donc d'être une autorité légitime aux fins de la LPRPDE.

Jusqu'à maintenant, j'ai expliqué la façon dont *Spencer* limite de façon importante la divulgation de renseignements au gouvernement par des organisations privées, mais tout ça dépend de l'existence ou de l'inexistence d'une attente raisonnable en matière de vie privée. Le tribunal ne dit rien au sujet des limites lorsqu'il existe une attente raisonnable en matière de vie privée.

Je souhaite que l'on traite de cette question de façon claire, puisque plusieurs joueurs importants participent au débat. Le ministre MacKay a dit qu'il n'est pas nécessaire de modifier le projet de loi à la suite de *Spencer*, et on en vient à se demander quel sera l'impact concret de l'arrêt *Spencer*.

De nombreux ministères à qui certains députés avaient demandé d'expliquer les circonstances dans lesquelles ils reçoivent des renseignements d'organisations privées n'ont pas répondu du tout, donc nous ne savons pas quel genre d'informations ils obtiennent. Certaines entreprises de télécommunications ont dit, à la suite de l'arrêt *Spencer*, qu'elles n'allaient plus fournir de renseignements au gouvernement, sauf dans les trois circonstances que j'ai énoncées, et d'autres n'ont pas réagi.

Il nous reste donc, à moi et aux Canadiens, un jugement très utile qui limite la divulgation de renseignements au gouvernement par des organisations privées lorsqu'il existe une attente raisonnable en matière de vie privée, ce qui laisse beaucoup de place à l'interprétation des différents intervenants concernant les contextes où il y a ou non une attente raisonnable en matière de vie privée.

Le sénateur McInnis : Merci beaucoup. Ce n'est pas ma question, mais les organisations d'application de la loi nous ont pratiquement dit que *Spencer* a fait taire les organisations privées. Elles ne divulguent plus rien. Mais ce n'est pas nécessairement une consolation.

I found a wonderful document entitled *A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century*, a reference document from the Office of the Privacy Commissioner of Canada, 2010. I found it very interesting. I was looking for a formula because you always want to try to find the sweet spot, the balance, between the privacy and the protection of Canadians. I didn't find the formula. I may have partially found one in one of the test cases.

The paragraph here is titled "privacy, security and the stakes for democracy."

> So what is at stake as policy makers and legislators grapple with the integration of privacy and public safety? . . . Foremost at stake for government is the issue of trust. Trust between citizens and their neighbours, as well as between citizen and the state, hinge on a mutual understanding about privacy, its value as both a human right and a collective good.

When I read that, I thought it was so accurate. I will read one more sentence that throws out the challenge to us.

> In conclusion, the main purpose of this document is to provide reference in the constantly evolving context of security to ensure that the fundamental right to privacy is protected.

When I looked at this, I said, "That's right." It's a moving target, and what governments have to try to do in that target is find the bull's eye, the sweet spot, where it is not injurious to the privacy of the individual but at the same time trying to protect Canadians.

Now, Bill C-13, used in this reference guide, I think hits the sweet spot. It hits the balance. On page 17 we find the four-part test — necessity, effectiveness, proportionality and alternatives. The reason I say it meets the test is that the gradual investigative powers that are given to police to find information are done so with judicial oversight every step of the way. As I said earlier to a witness, if they didn't have that reason to suspect, they wouldn't meet the test of reason to believe and the investigation would die.

The Chair: May I encourage you to put a question.

Senator McInnis: The question is first I want to thank you for this. That is the test, and I would like your comments on it because you put it out in the public domain to help us all, and you certainly helped me convince myself once again that Bill C-13 is the proper way.

Mr. Therrien: Thank you. Of course the challenge before you is to find the right balance, and in that balance the importance of the harm at play, which in part is cyber intimidation, is a factor,

J'ai découvert un document extraordinaire intitulé *Une question de confiance : Intégrer le droit à la vie privée aux mesures de sécurité au 21e siècle*. Il s'agit d'un document de référence du Commissariat à la protection de la vie privée du Canada publié en 2010. Je l'ai trouvé très intéressant. J'essayais de trouver la formule pour atteindre le point idéal, l'équilibre entre le respect de la vie privée et la protection des Canadiens. Je n'ai pas trouvé cette formule. J'ai peut-être trouvé une partie de la formule dans l'une des études de cas.

Le paragraphe suivant est intitulé « Vie privée, sécurité et les enjeux pour la démocratie ».

> Quels sont donc les enjeux en cause au moment où les décideurs et les législateurs doivent se pencher sur l'intégration du droit à la vie privée dans les initiatives de santé publique? [...] La question de la confiance est la plus importante pour le gouvernement. La confiance entre les citoyens et leurs voisins de même qu'entre les citoyens et l'État repose sur une compréhension mutuelle de la protection de la vie privée, de sa valeur en tant que droit de la personne et du bien commun.

Quand j'ai lu ce passage, je l'ai trouvé tellement exact. Je vais vous lire une autre phrase qui nous relance le défi.

> En conclusion, le présent document vise principalement à fournir une référence dans le contexte changeant de la sécurité de manière à ce que le droit fondamental à la vie privée soit protégé.

Quand j'ai lu ça, je me suis dit : « C'est exactement ça. » Il s'agit d'une cible mouvante, et les gouvernements doivent tenter de trouver le point de mire, le centre d'impact, où la protection des Canadiens ne nuit pas au respect de la vie privée de chacun.

Le projet de loi C-13, que l'on utilise dans ce guide de référence, atteint, selon moi, le point de mire. Il atteint l'équilibre. À la page 17, nous retrouvons le critère en quatre parties — nécessité, efficacité, proportionnalité et autres solutions possibles. La raison pour laquelle j'affirme que le projet de loi respecte le critère est que les pouvoirs d'enquête graduels qui sont donnés aux policiers afin de trouver des renseignements font l'objet d'un contrôle judiciaire à chaque étape du processus. Comme je l'ai dit plus tôt à un témoin, s'ils n'avaient pas de raison de soupçonner une personne, ils ne respecteraient pas le critère des raisons de croire, et l'enquête prendrait fin.

Le président : Je vous encourage à poser une question.

Le sénateur McInnis : Premièrement, j'aimerais vous remercier. Il s'agit du critère, et j'aimerais que vous le commentiez, puisque vous l'avez mis à la disposition du domaine public afin de nous aider tous, et vous m'avez certainement convaincu une fois encore que le projet de loi C-13 constitue la bonne solution.

M. Therrien : Merci. Bien sûr, le défi qui se présente à vous est de trouver l'équilibre, et l'importance du tort qui est en cause et qui est en partie constitué de la cyberintimidation est un facteur,

but Bill C-13 goes well beyond cyber intimidation. It provides new tools to law enforcement for any crime under the Criminal Code or any act of Parliament.

So I would encourage you to think about whether these powers, based on reasonable grounds to suspect, are always necessary, not only for cyberbullying but for all the crimes to which they apply, and I would suggest to you that that is not the proper balance.

Judicial oversight is certainly an important element. There is no question about that, but the courts generally have held that even when there is judicial oversight, the question of the threshold, the type of evidence required for the court to issue the order or the warrant sought should generally be reasonable grounds to believe, and there are very limited circumstances where the reasonable grounds to suspect standard is actually upheld.

I would suggest to you that there needs to be clear demonstration that reasonable grounds to suspect is necessary, and if you bear with me just for one more minute, I heard attentively the —

The Chair: I'm sorry; I can't give you another minute. We may get back to you on that depending how the time goes. Senator Joyal?

Senator Joyal: Welcome, Mr. Therrien, Mr. Caron and Ms. Kosseim.

I tried to understand what has changed between the time you testified in the House of Commons on this bill and what you propose as a recommendation to us today, to which I subscribe, by the way. Could you quickly run through what has changed about your position since *Spencer* that you have put into your recommendation?

Mr. Therrien: Thank you. A number of things have stayed the same from my submissions in June, including suggesting that thresholds be generally reasonable grounds to believe, but now I make a few more suggestions based on my reading of *Spencer* and the events around *Spencer* since it was released.

Spencer has, as I've explained to Senator Baker, significantly clarified an issue that was before the House of Commons when I appeared in June, which is how sensitive is the information that people put on the Internet that is subject to state powers requiring production of information; and at that time, it was a complete unknown, and many people were suggesting that the information sought in Bill C-13 was not sensitive, did not deserve constitutional protection, et cetera.

Now *Spencer* has clarified that significantly, provided that there is a reasonable expectation of privacy. And despite the judgment in *Spencer*, I see again important players in the debate

mais le projet de loi C-13 va bien au-delà de la cyberintimidation. Il fournit de nouveaux outils aux organisations d'application de la loi pour toute infraction au Code criminel ou aux lois du Parlement.

Je vous encourage donc à réfléchir à la question de savoir si ces pouvoirs, selon les motifs raisonnables de soupçonner, sont toujours nécessaires, non seulement pour la cyberintimidation, mais pour tous les crimes auxquels ils s'appliquent, et je vous dis que, selon moi, l'équilibre n'est pas là.

Le contrôle judiciaire constitue à coup sûr un élément important. Ça ne fait aucun doute, mais les tribunaux ont, de façon générale, soutenu que même lorsqu'il y a un contrôle judiciaire, la question du seuil, le type de preuve nécessaire pour que le tribunal émette une ordonnance ou un mandat devrait habituellement tenir aux motifs raisonnables de croire, et il y a des circonstances très particulières où la norme des motifs raisonnables de soupçonner est maintenue.

Je vous dirais qu'il faut démontrer clairement que les motifs raisonnables de soupçonner sont nécessaires, et, si vous voulez bien m'écouter pour une autre minute, j'ai écouté attentivement...

Le président : Je suis désolé; je ne peux pas vous donner une autre minute. Nous allons peut-être y revenir si le temps nous le permet. Sénateur Joyal?

Le sénateur Joyal : Bienvenue, monsieur Therrien, monsieur Caron et madame Kosseim.

J'ai tenté de comprendre ce qui a changé entre le moment où vous avez témoigné devant la Chambre des communes concernant ce projet de loi et aujourd'hui, où vous faites cette recommandation, recommandation que j'appuie, en passant. Pourriez-vous expliquer rapidement ce qui vous a fait changer d'opinion depuis *Spencer* et qui vous a fait modifier votre recommandation?

M. Therrien : Merci. Un certain nombre de choses n'ont pas changé depuis mon témoignage en juin, y compris ma suggestion que les seuils d'application soient, de façon générale, la présence de motifs raisonnables de croire, mais, maintenant, je fais quelques suggestions supplémentaires fondées sur la lecture de *Spencer* et sur les événements qui ont lieu depuis sa publication.

L'arrêt *Spencer* a, comme je l'ai expliqué au sénateur Baker, éclairci de façon importante un enjeu dont il était question à la Chambre des communes lorsque j'ai témoigné en juin, enjeu qui touchait à la nature délicate des renseignements que les gens mettent sur Internet qui sont sujets à l'autorité de l'État concernant la communication de renseignements; à ce moment, c'était complètement inconnu, et de nombreuses personnes laissaient entendre que les renseignements visés par le projet de loi C-13 n'étaient pas de nature délicate, ne nécessitaient pas de protection constitutionnelle, et cetera.

Maintenant, *Spencer* a éclairci ce point de façon importante, pourvu qu'il y ait une attente raisonnable en matière de vie privée. Et malgré le jugement rendu dans l'arrêt *Spencer*, je constate une

— government, telecommunication companies, federal departments — making statements that do not give me a whole lot of confidence on what impact *Spencer* will actually have. They seem to give a very narrow interpretation to *Spencer*.

The bill before you suggests that certain information would be obtained based on reasonable grounds to suspect. I'm advocating reasonable grounds to believe. But if the committee accepts reasonable grounds to suspect, one thing that I think would be useful to clarify is that the common law should no longer be relied upon to obtain information based on evidence lower than reasonable grounds to suspect. I cannot imagine really a standard lower than reasonable grounds to suspect.

If the common law is left to stand to authorize the type of requests that law enforcement make to telecommunication companies and others, based on the common law, based on an argument that there is no reasonable expectation of privacy, it means that information would be sought on something lower than reasonable grounds to suspect. I do not think that is a balanced way of approaching the issue.

Senator Joyal: Has it not been your position in the past that the lower the threshold the higher the control needs to be, as well as the need to notify the person? I was surprised that you didn't mention the need to notify the person that exists when you get a search warrant to wiretap a telephone line.

If you tap my computer and my telephone line, I will be better protected on my telephone line than on my computer because at some point in time you will have to inform me that you have tapped my telephone line. On the computer, you will go unnoticed. I won't even know that you have all the metadata. There is the report you published, which I think is a very good report, in which you analyze all the information you can get in the metadata, and you get much more information through my computer than just listening to my conversation with Senator Baker, and after that you will have to come and tell me that I have spoken to Senator Baker and you have received that information.

That's why I think there is no logic at this point in the system, and I'm trying to wrestle how we should make sure that the system remains logical and that the parameters are the same and that they are rational in terms of control at the various levels.

Patricia Kosseim, Senior General Counsel and Director General, Office of the Privacy Commissioner of Canada: Thank you for the question. We do advocate the inclusion of transparency and accountability mechanisms. We talk about public reporting, but certainly after-the-fact notice is a very important means of inserting accountability into the provisions. The Supreme Court has said so in *R. v. Tse* and more recently in *R. v. Wakeling*. Even

fois encore que d'importants intervenants qui participent au débat — le gouvernement, les entreprises de télécommunications, les ministères fédéraux — font des déclarations qui me laissent croire que *Spencer* n'aura peut-être pas un impact concret. Ils semblent interpréter *Spencer* de façon très étroite.

Le projet de loi qui vous est présenté laisse entendre que certaines informations seraient obtenues en fonction de motifs raisonnables de soupçonner. Je préconise les motifs raisonnables de croire. Mais si le comité accepte les motifs raisonnables de soupçonner, je crois qu'il serait utile de clarifier le fait qu'il n'est plus nécessaire de se fier au droit commun pour obtenir des renseignements à l'aide de preuves moins solides que des motifs raisonnables de soupçonner. Je ne peux pas envisager une norme moins élevée que les motifs raisonnables de soupçonner.

Si la common law doit autoriser le type de demandes que les organisations d'application de la loi font aux entreprises de télécommunications et aux autres types d'entreprises, selon la common law et l'argument selon lequel il n'y a pas d'attente raisonnable en matière de vie privée, cela signifie que les informations seraient obtenues à l'aide de preuves moins solides que des motifs raisonnables de soupçonner. Je ne crois pas qu'il s'agisse d'une façon équilibrée d'aborder l'enjeu.

Le sénateur Joyal : N'étiez-vous pas d'avis que plus le seuil d'application est bas, plus le contrôle doit être élevé, tout comme le besoin d'avertir la personne? Je suis surpris que vous n'ayez pas mentionné le besoin d'avertir la personne au moment de l'obtention d'un mandat pour mettre sur écoute une ligne téléphonique.

Si vous mettez mon ordinateur ou ma ligne téléphonique sous écoute, je serai mieux protégé sur ma ligne téléphonique que sur mon ordinateur, puisque, à un certain moment, vous devrez m'informer que vous avez mis ma ligne téléphonique sous écoute. Pour ce qui est de l'ordinateur, je n'en saurai jamais rien. Je ne saurai même pas que vous avez toutes mes métadonnées. Dans un rapport que vous avez publié, qui est, selon moi, un très bon rapport, vous analysez toute l'information que vous pouvez obtenir grâce aux métadonnées, et vous obtenez bien plus d'information par l'entremise de mon ordinateur qu'en écoutant ma conversation avec le sénateur Baker, et, après, vous allez devoir venir me voir et me dire que vous savez que j'ai parlé avec le sénateur Baker et que vous avez reçu cette information.

C'est pourquoi, selon moi, ce système n'est pas logique, et j'essaie de déterminer la manière dont nous devrions nous assurer que le système demeure logique, que les paramètres sont les mêmes et qu'ils sont rationnels au chapitre du contrôle à différentes échelles.

Patricia Kosseim, avocate générale principale et directrice générale, Commissariat à la protection de la vie privée du Canada : Merci pour la question. Nous défendons la transparence et les mécanismes d'imputabilité. Nous parlons des rapports publics, mais, sans aucun doute, le fait d'avertir après coup constitue une façon importante d'intégrer un élément d'imputabilité aux dispositions. La Cour suprême l'a dit dans

in *Wakeling* both the majority and the dissent confirmed that transparency and accountability, such as after-the-fact notice and public reporting, are important policy decisions that have to be considered precisely by Parliament. Both of them invite Parliament to consider these important mechanisms, and this is why we would encourage you today to consider this. Public reporting was our recommendation, but after-the-fact notice is a very important mechanism that could achieve the same means or the same ends.

Senator Frum: In the same report that Senator Joyal just referenced, the metadata and privacy report of October 2014 and on the theme of reasonable expectation of privacy, you lay out here what metadata is collected by the providers when you use the Internet and your telephone.

The issue that I'm struggling with on reasonable expectation of privacy — and I asked this of the criminal lawyer who appeared yesterday — is that your provider is already collecting the metadata. They're using it, and what I don't understand is when law enforcement receives a transmission-of-data warrant, they are going then to be receiving the same level of information about you that Google and Facebook already have, are already collecting and are already monetizing. They are already employing that information against you.

To this philosophical question about what is the reasonable expectation of privacy, as the user, my data is being collected, deployed, sold, monetized and capitalized already. When there is a reasonable suspicion, then law enforcement can have access to it as well, but my privacy is already being violated as is. No?

Mr. Therrien: You're raising a good question as to whether there are sufficient safeguards to protect personal information vis-à-vis private organizations and not the state. Based on our current law, this information is collected by Google and other companies based on consent, is the argument.

The individual uses certain services and consents to certain uses by the organization of that information. I would agree with you that private organizations with consent, whether it is fully informed or fully detailed, is another matter, but private organizations use this information for many purposes.

Legally, the issue here is consent. To what extent has this been consented to by the consumer receiving services from the private organization?

When the state knocks on the door of a private organization, we're no longer talking about consent, of course. We're talking about the state, for legitimate investigative purposes, wanting information without consent from the individual who is subject to

R. c. *Tse*, et, plus récemment, dans *R*. c. *Wakeling*. Même dans *Wakeling*, la majorité ainsi que les opposants ont confirmé que la transparence et l'imputabilité, comme l'avis après coup et les rapports publics, sont des décisions importantes en matière de politiques dont le Parlement doit tenir compte. Les deux groupes invitent le Parlement à tenir compte de ces mécanismes importants, et c'est pourquoi nous vous encourageons aujourd'hui à le faire. C'est nous qui avons recommandé les rapports publics, mais l'avis après coup est un mécanisme très important qui nous permettrait d'atteindre les mêmes objectifs à l'aide des mêmes moyens.

La sénatrice Frum : Dans le même rapport que celui dont le sénateur Joyal vient de parler, les rapports sur les métadonnées et sur la vie privée d'octobre 2014 qui traitent de l'attente raisonnable en matière de vie privée, vous précisez quelles métadonnées sont recueillies par les fournisseurs lorsque vous utilisez Internet et votre téléphone.

Ce qui me dérange au sujet de l'attente raisonnable en matière de vie privée — et j'ai posé cette question au criminaliste qui a témoigné hier —, c'est le fait que votre fournisseur recueille déjà les métadonnées. Il les utilise, et, ce que je ne comprends pas, c'est que lorsqu'une organisation d'application de la loi reçoit un mandat de transmission des données, elle va recevoir des renseignements à votre sujet que Google et Facebook possèdent, collectent et monétisent déjà. Ils utilisent déjà ces informations contre vous.

Qu'est-ce qui constitue une attente raisonnable en matière de vie privée lorsque, en tant qu'utilisatrice, mes données sont déjà recueillies, utilisées, vendues, monétisées et commercialisées? Lorsqu'elles ont des motifs raisonnables de soupçonner, les organisations d'application de la loi peuvent aussi y a voir accès, mais ma vie privée est déjà compromise, non?

M. Therrien : Vous soulevez une bonne question : la protection des renseignements personnels à l'égard des organisations privées, et non à l'égard de l'État, est-elle suffisante? Selon notre législation actuelle, les renseignements recueillis par Google et d'autres entreprises sont recueillis avec notre consentement, c'est le principal argument invoqué.

Une personne utilise certains services et consent à ce que l'organisation utilise ses renseignements de certaines façons. Je suis d'accord avec vous : les organisations privées ont notre consentement; c'est une autre question de savoir s'il est bien informé ou détaillé, mais les organisations privées utilisent ces renseignements à de nombreuses fins.

Juridiquement, la question tient au consentement. À quel point le consommateur qui reçoit des services a-t-il consenti à l'utilisation de ses renseignements par l'organisation privée?

Lorsque l'État cogne à la porte d'une organisation privée, nous ne parlons plus de consentement bien sûr. Nous parlons de l'État qui, à des fins légitimes d'enquête, veut obtenir des renseignements sans le consentement de la personne à laquelle

it. That is why we have, I would suggest, rules on what are the limited circumstances in which this should be permitted at law, and generally reasonable grounds to believe is the appropriate threshold.

Senator Frum: I would question how much consent there is on the collection of that data. I think it's forced consent.

Mr. Therrien: That's a fair question.

Senator Frum: You can't use services unless you agree, and so I'm not sure about that.

Again, on the expectation of privacy, once I have allegedly consented to the collection of that data, I'm acknowledging that it's not private anymore.

Mr. Therrien: You're acknowledging that the private organization can use it for the purposes for which it sought consent. Let's remember that the Supreme Court in *Spencer* addressed the issue of anonymity on the Internet and of a reasonable expectation. In that case the court made clear that the information in question, personal information going to the activities of an individual, does attract a reasonable expectation of privacy as a constitutional matter. That is now settled law, and that comes with certain consequences.

As a matter of constitutional law, this is now settled. It was not settled in June. It is now settled.

You're raising very fair questions as to how informed, voluntary and fulsome the consent provided to a private organization is. I totally agree with that, but I think there's a big difference between collection and use by private organizations and compulsory obtainment of information by the state for criminal purposes.

[*Translation*]

Senator McIntyre: Thank you for your presentation, Mr. Therrien. I looked at the bill and my understanding is that there are two major components: first, law enforcement officers are required to apply for warrants, and second, there is judicial discretion on whether or not to issue a warrant.

In other words, law enforcement has the obligation to report the facts to the judge of first instance, who then has the information to conduct a proper review and decide whether or not a warrant needs to be issued.

I see that the only section that does not require a warrant is the one dealing with preservation. That being said, "preservation" does not mean "protection" and, as a result, I think the bill strikes a balance between the protection of privacy and the protection of the public.

I would like to hear what you have to say on that.

ils se rattachent. C'est pourquoi nous avons, je dirais, des règles sur ce qui limite les circonstances dans lesquelles cela est permis, et les motifs raisonnables de croire constituent le seuil approprié.

La sénatrice Frum : Je me demande à quel point le consentement est donné pour la collecte de ces données. Je crois qu'il s'agit d'un consentement forcé.

M. Therrien : La question se pose.

La sénatrice Frum : Vous ne pouvez pas utiliser le service sans donner votre consentement, donc je ne suis pas vraiment certaine.

Au sujet de l'attente en matière de vie privée, une fois que j'ai supposément consenti à la collecte de ces données, je reconnais qu'elles ne sont plus privées.

M. Therrien : Vous reconnaissez que l'organisation privée peut les utiliser aux fins pour lesquelles elle a demandé de consentir. Souvenons-nous que la Cour suprême, dans l'arrêt *Spencer*, a traité de l'enjeu de l'anonymat sur Internet et de l'attente raisonnable. Dans ce cas, le tribunal a clairement établi que les renseignements en question, les renseignements personnels concernant les activités d'une personne, sont sujets à une attente raisonnable en matière de vie privée d'un point de vue constitutionnel. Il s'agit désormais d'un principe juridique établi, et cela a certaines conséquences.

D'un point de vue constitutionnel, le principe juridique est établi. Il ne l'était pas en juin, mais il l'est maintenant.

Vous soulevez des questions très légitimes sur la mesure dans laquelle le consentement donné à une organisation privée est éclairé, volontaire et complet. Je suis tout à fait d'accord avec cela, mais je crois qu'il y a une grande différence entre le fait pour une organisation privée de recueillir et d'utiliser des renseignements et la collecte obligatoire de renseignements par l'État à des fins pénales.

[*Français*]

Le sénateur McIntyre : Merci pour votre présentation, monsieur Therrien. En examinant le projet de loi, je comprends qu'il constitue deux volets importants : tout d'abord, l'obligation de la part des forces de l'ordre de faire une demande pour obtenir un mandat; de plus, la discrétion judiciaire d'émettre ou de ne pas octroyer un mandat.

Autrement dit, les forces de l'ordre ont l'obligation de rapporter les faits au juge de première instance et, armé de ces faits, le juge de première instance est dans une excellente position pour en faire la révision et décider s'il va lancer un mandat ou non.

Je remarque que le seul article qui ne requiert pas de mandat est celui qui concerne la préservation. Cela étant dit, « préservation » ne signifie pas « protection » et, pour cette raison, je crois que le projet de loi protège l'équilibre entre la protection de la vie privée et la protection du public.

J'aimerais connaître votre opinion sur ce sujet.

Mr. Therrien: In terms of preservation orders, we agree that the reasonable suspicion standard is adequate in this case. As you say, it is one thing to preserve information that might eventually be useful in a police investigation, and it is a whole different thing to disclose the information to police forces.

We agree that preservation orders are issued on reasonable suspicion grounds. However, despite the judicial oversight, we feel that the reasonable grounds to believe standard should apply to disclosing information to police forces. That is what courts have generally been upholding for years.

Senator McIntyre: Thank you, Mr. Therrien.

[*English*]

Senator Batters: Thank you all for being here. Mr. Therrien, I think the last time we had a chance to speak was when you were in the Senate Chamber for your confirmation hearings or what have you.

Mr. Therrien: I remember well.

Senator Batters: Just because there's been so much talk over the last couple days especially about *Spencer*, I thought it might provide some interesting context to many on this committee who know these details, and I'm sure Mr. Therrien knows them well. For those who might be following this particular Bill C-13 hearing, it might be interesting for them to know a few of the facts behind the *Spencer* case.

In this case, in June 2014, the Supreme Court of Canada released its decision in *R v. Spencer*. I find this important to bring up, particularly because Saskatchewan is my home province and this is a Saskatchewan case.

In this case, Saskatoon police were able to identify Shaw Communications as the service provider of a person accessing and distributing child pornography. Police had used a law enforcement request, known as an LER, to obtain the basic subscriber information from Shaw that led to Mr. Spencer. Most of Canada's telecommunications services providers comply with LERs, and those are only made in relation to child sexual exploitation cases. Shaw did voluntarily provide that information, and the police then sought and obtained a search warrant to seize Mr. Spencer's computer.

The accused then challenged that LER on the basis of a reasonable expectation of privacy in an IP address. The Saskatchewan Court of Appeal and the Saskatchewan Court of Queen's Bench initially upheld the use of that for basic subscriber information, saying there was no reasonable expectation of privacy in the information attached.

M. Therrien : Sur la question des ordonnances de préservation, nous sommes d'accord que la norme du soupçon raisonnable est adéquate dans ce cas. Comme vous le dites, c'est une chose de préserver des renseignements qui pourraient être utiles à une enquête policière éventuellement, et c'en est une tout autre de divulguer des renseignements aux corps policiers.

Nous sommes d'accord pour dire que les ordonnances de préservation sont émises sur la base des soupçons raisonnables. Cependant, malgré le contrôle judiciaire, on pense que, à l'étape de la divulgation des renseignements aux forces policières, c'est la norme des motifs raisonnables de croire qui devrait s'appliquer, comme les tribunaux l'ont reconnu, généralement, depuis des années.

Le sénateur McIntyre : Merci, monsieur Therrien.

[*Traduction*]

La sénatrice Batters : Merci à vous tous d'être venus ici. Monsieur Therrien, je crois que la dernière fois où nous avons eu la chance de discuter avec vous, c'était quand vous étiez au Sénat pour votre audience d'approbation, ou quelque chose comme ça.

M. Therrien : Je m'en souviens bien.

La sénatrice Batters : Étant donné qu'on a tellement parlé, depuis quelques jours, de *Spencer*, en particulier, j'ai pensé que cette affaire pourrait fournir un contexte assez intéressant aux nombreux membres du comité qui en connaissent les détails, et je suis sûre que M. Therrien les connaît bien. Pour ceux qui suivent les audiences sur le projet C-13, il serait peut-être intéressant de connaître un peu les faits de l'affaire *Spencer*.

En juin 2014, la Cour suprême du Canada a rendu sa décision dans *R. c. Spencer*. Je trouve qu'il est intéressant d'en parler, en particulier parce que la Saskatchewan est ma province natale et qu'il s'agit d'une affaire qui s'est déroulée en Saskatchewan.

Dans cette affaire, la police de Saskatoon a été en mesure de déterminer que Shaw Communications était le fournisseur de services d'une personne qui faisait circuler de la pornographie juvénile. La police a présenté une demande de communication afin d'obtenir de Shaw les renseignements de base sur l'abonné qui lui ont permis de remonter jusqu'à M. Spencer. La plupart des fournisseurs de services de télécommunications du Canada respectent les demandes de communication, et ces dernières ne sont présentées que lorsqu'il s'agit d'exploitation sexuelle des enfants. Shaw a fourni de bon gré ces renseignements, et la police a ensuite demandé et obtenu un mandat de perquisition afin de s'emparer de l'ordinateur de M. Spencer.

L'accusé a par la suite contesté la demande de communication en invoquant l'attente raisonnable de protection en matière de vie privée relativement à son adresse IP. Au départ, la Cour d'appel de la Saskatchewan et la Cour du Banc de la Reine de la Saskatchewan avaient soutenu qu'il était possible de s'en servir pour obtenir des renseignements de base sur les abonnés, affirmant qu'aucune attente raisonnable de protection en matière de vie privée n'était liée à ces renseignements.

The Supreme Court of Canada then dismissed the appeal, actually, and confirmed the conviction of possession of child pornography, which some following this might find interesting, but they ordered a new trial, given that they said that the trial judge had erred in interpreting the offence of making available child pornography under the Criminal Code.

The court concluded that Mr. Spencer enjoyed a reasonable expectation of privacy in his identity in respect of his anonymous online activities, and the actions of the police constituted a search.

Another interesting finding is that the Supreme Court of Canada also ruled that the evidence in question in the *Spencer* case, in particular, should not be excluded on the basis of subsection 24(2) of the Charter analysis, as articulated in *Grant*.

I just wanted to draw that to people's attention to bring the facts out. As lawyers, we sometimes toss out these case names without knowing what the facts of the case are.

The Chair: We are running a little over time, so we're not going to have an opportunity for second round. Mr. Therrien and your staff, we very much appreciate your appearance here today and your testimony.

For our final panel this afternoon, from the Boys and Girls Clubs of Canada, we have Rachel Gouin, Director, Research and Public Policy; and Fahd Alhattab, who is an alumnus of the organization. From the Bully Free Community Alliance, we have Basiliki Schinas-Vlasis, Co-Founder; and Gwyneth Anderson, also Co-Founder.

Welcome, all. I haven't been given any indication of who is going to give the opening statements. We'll let you make the call. Please proceed.

Fahd Alhattab, Alumnus, Boys and Girls Clubs of Canada: Thank you for having us.

A little bit about me. I'm a Boys and Girls Clubs of Canada and Ottawa alumnus. I've been going to the Boys and Girls Clubs for 12 years, a place where my brothers and sisters and I kind of grew up.

Thank you for having us here today to speak about Bill C-13. The Boys and Girls Clubs of Canada is dedicated to supporting the growing and development of children and youth all across Canada. We serve about 200,000 young people every year, in 650 different communities, something we're very proud of. We're excited to be able to speak to this.

There are four sections that I'll be speaking about and topics to cover: protection and privacy rights; the consultation with youth; education; and restorative justice.

La Cour suprême du Canada a alors rejeté l'appel, en fait, et confirmé la condamnation pour possession de pornographie juvénile, ce que certaines personnes qui suivent l'affaire pourraient trouver intéressant, mais a ordonné un nouveau procès, jugeant que le juge de première instance avait erré dans l'interprétation de l'infraction de distribution de pornographie juvénile aux termes du Code criminel.

Le tribunal a conclu que M. Spencer pouvait raisonnablement s'attendre à une protection en matière de vie privée touchant ses activités anonymes en ligne et que les actes de la police constituaient une perquisition.

Autre conclusion intéressante, la Cour suprême du Canada a également déclaré que les éléments de preuve en question, dans *Spencer*, en particulier, ne devraient pas être écartés en application du paragraphe 24(2) de la Charte, comme on l'avance dans *Grant*.

Je voulais tout simplement attirer votre attention sur ces faits. En tant qu'avocats, nous avons parfois tendance à lancer ces noms en l'air, sans vraiment connaître les faits de l'affaire.

Le président : Nous manquons un peu de temps, alors il nous sera impossible de faire une deuxième série de questions. Nous apprécions beaucoup, monsieur Therrien et vos collègues, que vous soyez venus témoigner ici aujourd'hui.

Nos derniers témoins cet après-midi représentent les Clubs Garçons et Filles du Canada. Nous recevons Rachel Gouin, directrice, Recherche et politiques publiques, et Fahd Alhattab, qui est un ancien membre de l'organisation. Ensuite, nous accueillons Basiliki Schinas-Vlasis et Gwyneth Anderson, cofondatrices de la Bully Free Community Alliance.

Bienvenue tout le monde. On ne m'a pas indiqué qui allait prononcer une déclaration préliminaire. Je vais vous laisser en décider. Veuillez commencer.

Fahd Alhattab, ancien membre, Clubs Garçons et Filles du Canada : Merci de nous recevoir.

Je vais vous parler un peu de moi. Je suis un ancien membre des Clubs Garçons et Filles du Canada et d'Ottawa. Je vais aux Clubs Garçons et Filles depuis 12 ans, alors on peut dire en quelque sorte que mes frères et mes sœurs et moi-même avons grandi dans ces clubs.

Merci de nous recevoir aujourd'hui pour discuter du projet de loi C-13. Les Clubs Garçons et Filles du Canada ont pour objectif de soutenir la croissance et le développement des enfants et des jeunes de toutes les régions du Canada. Nous nous occupons chaque année d'environ 200 000 jeunes, dans 650 collectivités, et nous sommes très fiers de ce que nous accomplissons. Nous sommes emballés de pouvoir discuter de cette question.

Mon exposé compte quatre volets qui portent sur les sujets suivants : le droit à la protection et à la vie privée, la consultation des jeunes; l'éducation; et la justice réparatrice.

To begin around protection and privacy rights, we are very much for Bill C-13 and the fact that it protects the children and youth that we work with around cyberbullying. Young people deserve protection from cyberbullying, but they also deserve protection from unreasonable interference with their privacy. While matters of privacy are not our expertise, they ought to be given a proper consideration.

The only recommendation we have around protection and privacy right is to, obviously, listen to the Privacy Commissioner and note that, protecting children from cyberbullying while protecting their right to privacy.

The second part is around consultation with youth. As most of you know, youth are connected in so many different ways. Ninety-nine per cent of youth across Canada are connected to the Internet outside of school. Eighty-five per cent of youth in grade 11 have access to cellphones. Through their use of technology, youth are testing social boundaries. This is their way of experimenting as teenagers, of getting to know different things. It's part of the way that they're growing up. In addressing cyberbullying, legislators would benefit from understanding how children and youth use technology and what they think will work in addressing cyberbullying.

Our recommendation here is to consult youth on the legislation, on prevention programs and on education that addresses cyberbullying, to ensure that the efforts to stop the distribution of non-consensual images are informed by those who are most affected by it.

The third part is around education. The desire to address bullying and cyberbullying has resulted in a patchwork of legislation across federal, provincial and territorial jurisdictions. As you know, the Internet does not have borders the way countries and provinces do. We've put children and youth at risk of being confused about their responsibilities and the legal repercussions of their actions.

The Standing Senate Committee on Human Rights and the CCSO Cybercrime Working Group both recommended that the federal government play a leading role in coordinating efforts to address cyberbullying, in part through a national prevention strategy and legal education. We want to put this forth again and say that this is very important to us. The recommendation here is to lead the coordination of legislative efforts across all jurisdictions.

Pour commencer, en ce qui concerne le droit à la protection et à la vie privée, nous sommes très favorables au projet de loi C-13, étant donné qu'il protège les enfants et les jeunes avec qui nous travaillons dans le dossier de la cyberintimidation. Les jeunes ont le droit d'être protégés contre la cyberintimidation, mais ils ont également le droit d'être protégés contre toute atteinte déraisonnable à leur vie privée. Même si nous ne sommes pas des experts des questions relatives à la vie privée, il faut y accorder une considération appropriée.

Notre seule recommandation touchant le droit à la protection et à la vie privée est, bien sûr, qu'il faut écouter ce que dit le commissaire à la protection de la vie privée et se préoccuper de protéger les enfants contre la cyberintimidation tout en protégeant leur droit à la vie privée.

Le second volet concerne la consultation des jeunes. Comme la plupart d'entre vous le savez, les jeunes communiquent entre eux de très nombreuses manières. Quatre-vingt-dix-neuf pour cent des jeunes du Canada sont connectés à Internet, à l'extérieur de l'école. Quatre-vingt-cinq pour cent des jeunes de 11e année ont accès à un téléphone cellulaire. En utilisant la technologie, les jeunes mettent à l'épreuve les limites sociales. C'est de cette manière que les adolescents font leurs expériences, qu'ils apprennent à connaître différentes choses. C'est entre autres de cette façon qu'ils gagnent de la maturité. Au moment de s'attaquer à la cyberintimidation, les législateurs auraient avantage à comprendre comment les enfants et les jeunes utilisent la technologie et à savoir ce qui, à leur avis, aiderait à contrer la cyberintimidation.

Notre recommandation, ici, est de consulter les jeunes au sujet de la loi, des programmes de prévention et de l'éducation visant à lutter contre la cyberintimidation, pour s'assurer que les efforts visant à mettre fin à la distribution sans consentement d'images soient orientés par ceux qui sont le plus touchés.

Le troisième volet touche l'éducation. Le désir de lutter contre l'intimidation et la cyberintimidation a entraîné l'adoption d'un ensemble hétéroclite de lois par les gouvernements fédéral, provinciaux et territoriaux. Comme vous le savez, Internet n'a pas de frontières, contrairement aux pays et aux provinces. Nous faisons courir aux enfants et aux jeunes le risque d'être déroutés en ce qui concerne leurs responsabilités et les répercussions juridiques de leurs actes.

Le Comité sénatorial permanent des droits de la personne et le Groupe de travail sur la cybercriminalité du Comité de coordination des hauts fonctionnaires ont tous deux recommandé que le gouvernement fédéral joue un rôle de premier plan pour ce qui est de coordonner les efforts de lutte contre la cyberintimidation, en s'appuyant en partie sur une stratégie nationale de prévention et sur la sensibilisation aux aspects juridiques. Nous voulons réitérer cette demande et insister sur le fait que cet aspect nous importe énormément. Notre recommandation est d'assurer la direction de la coordination des efforts de tous les ordres de gouvernement.

The second recommendation would be to engage youth in developing a federal plan to educate young Canadians about cyberbullying and the law and to encourage respectful online communications. Obviously, with the Boys and Girls Clubs, with 650 communities, we say that we are open to being able to help deliver that education and work with the youth across the country.

In terms of restorative justice, given the number of young children navigating the Internet and interacting using digital communications, the government ought to consider enforcement measures that are age appropriate and that prioritize restorative justice. In the study on cyberbullying, the Standing Senate Committee on Human Rights also recommended that the promotion of restorative justice initiatives be a key component of any coordinated strategy to address cyberbullying developed, in partnership, by the federal, provincial and territorial governments.

We understand, as the Boys and Girls Clubs, that restorative justice is key to the way that we work. It's a main principle of the Youth Criminal Justice Act, and Boys and Girls Clubs in Alberta, British Columbia, Yukon and Ontario have all been offering youth restorative justice programs since 2001, with great success.

Our recommendation here, given the persuasive use of cellphones, social media and the Internet among children and youth, is to allow youth to take the responsibility for their actions and repair the harm they have done by favouring a restorative justice approach in all but most severe cases.

In conclusion, the Boys and Girls Clubs of Canada supports the government's efforts to criminalize the sharing of intimate images without consent and encourages the government to also ensure that privacy rights of youth are protected in the process. Most importantly, we urge the government to seek meaningful youth engagement and leadership in all matters pertaining to the development of legislation, policies and programs that affect youth. Organizations like ours can accompany youth to participate in forming decisions in bills, such as Bill C-13, and we encourage the government and the committee to reach out for support.

Basiliki Schinas-Vlasis, Co-Founder, Bully Free Community Alliance: Good morning, and thank you for inviting us here today to speak about Bill C-13. My name is Bessie Vlasis, and together with my colleague, Gwyneth Anderson, I am the co-founder of Bully Free Community Alliance, a not-for-profit, grassroots organization located in York Region, Ontario. Our organization advocates for students and families who have been affected by

La seconde recommandation serait de faire participer les jeunes à l'élaboration d'un plan fédéral d'éducation des jeunes Canadiens au sujet de la cyberintimidation et du droit et d'encourager le respect dans les communications en ligne. De toute évidence, les Clubs Garçons et Filles, qui sont présents dans 650 collectivités, sont ouverts à la possibilité d'aider à mettre en œuvre ces initiatives d'éducation et à travailler auprès des jeunes de tout le pays.

En ce qui concerne la justice réparatrice, étant donné le nombre de jeunes qui naviguent sur Internet et interagissent à l'aide des communications numériques, le gouvernement devrait envisager la création de mesures d'application de la loi qui sont appropriées à leur âge et mettre en priorité la justice réparatrice. Dans son étude sur la cyberintimidation, le Comité sénatorial permanent des droits de la personne recommandait également de faire de la promotion des initiatives axées sur la justice réparatrice un élément clé de toute stratégie coordonnée de lutte contre la cyberintimidation élaborée en partenariat par les gouvernements fédéral, provinciaux et territoriaux.

En tant que représentants des Clubs Garçons et Filles, nous comprenons que la justice réparatrice est la clé du travail que nous faisons. C'est un des grands principes de la Loi sur le système de justice pénale pour les adolescents, et les Clubs Garçons et Filles de l'Alberta, de la Colombie-Britannique, du Yukon et de l'Ontario offrent tous des programmes de justice réparatrice aux jeunes, depuis 2001, et obtiennent de très bons résultats.

Notre recommandation, en ce qui a trait à l'usage constant des téléphones cellulaires, des médias sociaux et d'Internet par les enfants et les jeunes, est de permettre aux jeunes de prendre la responsabilité de leurs actes et de réparer les torts qu'ils causent en favorisant une approche axée sur la justice réparatrice dans tous les cas, sauf les plus graves.

En conclusion, les Clubs Garçons et Filles du Canada soutiennent les efforts mis en œuvre par le gouvernement pour criminaliser la diffusion d'images intimes sans consentement, et ils encouragent le gouvernement également à s'assurer, ce faisant, que les droits des jeunes à la vie privée sont protégés. Mais, plus important encore, nous lui demandons instamment de chercher à mobiliser les jeunes de manière fructueuse et à rechercher leur orientation dans tous les dossiers relatifs à l'élaboration de lois, de politiques et de programmes qui touchent les jeunes. Des organismes comme le nôtre peuvent aider les jeunes à participer et à prendre position sur divers projets de loi, comme le projet de loi C-13, et nous encourageons le gouvernement et votre comité à demander leur soutien.

Basiliki Schinas-Vlasis, cofondatrice, Bully Free Community Alliance : Bonjour, et merci de nous avoir invitées ici aujourd'hui à discuter du projet de loi C-13. Je m'appelle Bessie Vlasis et, avec ma collègue Gwyneth Anderson, je suis la cofondatrice de la Bully Free Community Alliance, un organisme communautaire sans but lucratif dont les bureaux sont situés dans la région de York, en Ontario. Notre organisation défend les droits des étudiants et des

bullying, and we educate and bring awareness about bullying throughout our community and beyond. Our mission and vision is to build and sustain positive communities.

Our work began over eight years ago, when our children became victims of bullying. We realized quickly that there was not enough support for victims and their families. As our organization developed, our main concerns were technology and mental health. For all of the positive attributes, technology is being used to inflict harm and socially victimize. Cyberbullying has become an epidemic within our schools and communities, and, as technology evolves at a rapid pace, so will new ways to abuse it.

Snapchat, Instagram, Twitter, Tinder and Kik are just some of the apps and sites our youth visit, post to and download from. They are the 24-hour accessible apps and sites that subject our children to teasing, taunting, torment and threats, from which the only escape for some has been suicide.

It's easy to say to a teenager, "Just turn it off. Don't look at it, or don't read it," but the reality is very much tied to what they see and hear on the Internet and on social media. The number of "likes" they get on Instagram or re-tweets on Twitter are a large part of how they socialize today and where they draw their sense of value and belonging from.

We teach our children, as they grow up, not to talk to strangers and not to open the door to people they don't know, and yet we allow them to surf the Internet on social media sites in the privacy of their bedrooms, virtually allowing strangers to enter their lives in a potentially predatory and dangerous manner. Some children do not have the social and emotional maturity or life experience to understand that they could be putting themselves in harm's way.

We understand the privacy concerns that surround Bill C-13. However, when our children, or even adults, press an app or sign onto a social website, we have to ask the question: Do we really have privacy? The Criminal Code must be updated in order for our law enforcement to respond effectively and quickly when cybercrime occurs. Our society has changed, and our legislation needs to change with it.

The goal is to give our law enforcement the tools to combat cybercrime, allowing them access to data quickly to ensure the safety of our youth. We need to educate youth on the hazards of

familles qui ont été touchés par l'intimidation, et nous nous occupons d'éducation et de sensibilisation sur l'intimidation dans toute notre collectivité et au-delà. Notre mission et notre vision consistent à mettre sur pied et à soutenir des collectivités positives.

Notre travail a commencé il y a huit ans, lorsque nos enfants sont devenus des victimes de l'intimidation. Nous avons vite compris qu'il n'existait pas suffisamment de soutien pour les victimes et leur famille. Notre organisation a grandi peu à peu et nos principales préoccupations sont devenues la technologie et la santé mentale. Malgré toutes ses qualités, la technologie est utilisée pour causer du tort et pour faire des victimes dans la société. La cyberintimidation est devenue une épidémie dans nos écoles et dans nos collectivités et, comme la technologie évolue à un rythme rapide, les façons de causer du tort évolueront elles aussi.

Snapchat, Instagram, Twitter, Tinder et Kik ne sont que quelques exemples des applications et des sites que nos jeunes visitent et où ils affichent et téléchargent des choses. Ces sites et ces applications sont accessibles 24 heures sur 24, et c'est là que nos enfants se font taquiner, narguer, tourmenter et menacer, et la seule façon pour certains d'entre eux d'échapper à tout cela, c'est de se suicider.

Il est facile de dire à un ado de tout simplement éteindre son appareil, de ne pas regarder ces sites, de ne pas les lire. Mais la réalité est liée très étroitement à tout ce qu'ils voient et entendent sur Internet et dans les médias sociaux. Le nombre de « J'aime » qu'ils reçoivent sur Instagram ou sur Twitter fait largement partie de la façon dont les jeunes socialisent, aujourd'hui, et de la façon dont ils construisent leur estime de soi et leur sentiment d'appartenance.

Nous enseignons à nos enfants, quand nous les élevons, à ne pas parler aux étrangers et à ne pas ouvrir la porte à des gens qu'ils ne connaissent pas; pourtant, nous les laissons naviguer sur Internet et sur les sites des médias sociaux dans l'intimité de leur chambre, en permettant virtuellement à des étrangers d'entrer dans leur vie, par des moyens potentiellement dangereux et prédatoires. Certains enfants n'ont pas la maturité sociale et émotionnelle nécessaires ni une assez bonne expérience de la vie pour comprendre qu'ils peuvent ainsi se jeter dans la gueule du loup.

Nous comprenons les préoccupations relatives à la vie privée en ce qui a trait au projet de loi C-13. Cependant, lorsque nos enfants, ou même des adultes, utilisent une application ou s'inscrivent sur un site social en ligne, nous devons nous poser la question suivante : avons-nous vraiment une vie privée? Le Code criminel doit être mis à jour si l'on veut que les forces de l'ordre puissent réagir efficacement et rapidement à la cybercriminalité. Notre société a changé, et il faut que nos lois changent en même temps.

L'objectif est de donner à nos organismes d'application de la loi les outils nécessaires pour lutter contre la cybercriminalité, leur donner les moyens d'accéder rapidement aux données de façon à

misusing technology. We need to have stringent laws for those who purposefully use technology to harm and we need to hold predators and criminals accountable.

Gwyneth Anderson, Co-Founder, Bully Free Community Alliance: Bill C-13 is a positive and necessary step forward, but we can't stop here. We need to follow it with a national strategy. What would a national strategy look like? Provinces working together, using common language, through education, awareness and supports and laws, particularly with a focus on youth mental health and suicide.

Data must be regulated on cellphones for youth 12 and under. With full data on a cellphone, children as young as 6 have access to anything they want on the Internet at any time, often with no boundaries and no limits. They need to be protected from this.

We need to continue to develop the Get Cyber Safe website, as well as other websites, so that current information, supports and resources can be easily accessible and available.

We need continued public service announcements, similar to the ones currently running, so education on new legislation can be understood.

Bullying and being mean is learned behaviour. We do need a culture shift. We must initiate steps to promote a culture of respect and kindness for each other. This might sound like an unrealistic and impossible undertaking, but I'd like us to reflect for a moment. We changed a culture on drinking and driving, and we changed laws because it was killing people. We changed a culture on smoking because it was killing people, and we needed to change laws. We changed a culture on how we treat the environment. Laws were changed because people were getting sick and dying. We can certainly change a culture on how we treat each other. It can be done.

We have collaborated with our local school boards and police on a YouTube video, which you recently received via email through the clerk, called #yeswewill Change the Culture of Cyberbullying. We need this culture shift. It's a huge undertaking, but that should not discourage the effort.

assurer la sécurité de nos jeunes. Nous devons éduquer les jeunes sur les dangers d'une mauvaise utilisation de la technologie. Nous avons besoin de lois sévères pour ceux qui, intentionnellement, utilisent la technologie pour commettre des méfaits, et nous devons tenir les prédateurs et les criminels responsables.

Gwyneth Anderson, cofondatrice, Bully Free Community Alliance : Le projet de loi C-13 est un pas en avant positif et nécessaire, mais nous ne devons pas nous arrêter là. Nous devons l'accompagner d'une stratégie nationale. À quoi ressemblerait une stratégie nationale? Des provinces qui travaillent de concert, qui parlent la même langue, qui s'appuient sur l'éducation, la sensibilisation, le soutien et la loi, et qui mettent un accent particulier sur la santé mentale des jeunes et sur le suicide.

Il faut que les données des téléphones cellulaires pour les jeunes âgés de 12 ans ou moins soient réglementés. Avec des données complètes, un enfant d'aussi peu que six ans peut avoir accès, à partir d'un téléphone cellulaire, à tout ce qu'il veut, sur Internet, en tout temps, souvent sans aucune frontière ni limite. Il faut les protéger contre cela.

Nous devons continuer à promouvoir le site web Pensez cybersécurité, et d'autres sites web, de façon que l'information à jour, les services de soutien et les ressources soient facilement accessibles et disponibles.

Nous devons continuer à diffuser des messages d'intérêt public, semblables à ceux qui sont actuellement diffusés, de façon que l'information sur la nouvelle loi soit comprise.

L'intimidation et la méchanceté sont des comportements acquis. Nous devons effectuer un changement culturel. Nous devons prendre des mesures pour promouvoir une culture du respect et de la gentillesse à l'égard d'autrui. Cela pourrait sembler une entreprise irréaliste et impossible, mais j'aimerais que nous y réfléchissions un instant. Nous avons changé la culture touchant l'alcool au volant, et nous avons changé des lois parce que l'alcool au volant tuait des gens. Nous avons changé la culture touchant le tabagisme, parce que cela tuait des gens, et nous avons dû changer des lois. Nous avons changé la culture en matière d'environnement. Nous avons changé des lois parce que les gens tombaient malades et mourraient. Nous pouvons certainement changer la culture en ce qui concerne nos relations avec autrui. C'est possible.

Nous avons travaillé de concert avec les commissions scolaires locales et les services de police pour produire une vidéo sur YouTube, que vous avez récemment reçue dans un courriel du greffier; la vidéo porte le titre #yeswewill Change the Culture of Cyberbullying. Nous avons besoin de ce changement de culture. C'est une énorme entreprise, mais nous ne devons pas nous décourager.

It is not a child's privilege to feel safe at home, at school and in their community; it's their right — a very basic right. When children start taking their own lives and mental illness is at a national high, we the adults need to pay attention and take action. We hope you will join us in this vision.

The Chair: Thank you all. We will begin the questions with Senator Baker, the committee's deputy chair.

Senator Baker: Thank you to the presenters here today. These are excellent presentations, with excellent suggestions being made, and I'm glad these two presentations are now on the record of the Senate.

I don't have any specific questions to ask except perhaps that I don't know if you wish to elaborate on point number 2 by the last presenter, under the heading "What would a national strategy look like?" You said that the data must be regulated on cellphones for youth 12 and under because with full data on a cellphone, children as young as 6 have access to anything they want on the Internet at any time, often with no boundaries and no limits, and they need to be protected.

Do you want to elaborate on that? You don't have to, but do you wish to?

Ms. Anderson: We totally can. We work so much with front-line workers, with families and students, with teachers, so we get a lot of our information directly from teachers who are teaching in the classroom who have children as young as 6 coming to school with an iPhone, with full data, and access to anything they want at any time. Kids don't have the social and emotional maturity at that age to know that they're being groomed for something or to know that they're going on a site that they shouldn't go on. We would like to see at least some discussion on regulating something for children, because when parents purchase packages it's usually some type of text and data package. That's not to say they can't go home and get on the computer, but it's more the situation that computers are bigger and hopefully they're in a good area in a house where they have to log on and parents can see the screen. But when they're walking with handheld devices, we thought a discussion of what we could do to help protect our children who are very young from predators or from possibly getting themselves into situations that they can't get out of.

Senator Baker: You're suggesting we open up the dialogue, open up the subject on how we would approach this, as you mentioned, for those under a certain age limit.

Pour un enfant, ce n'est pas un privilège que de se sentir en sécurité à la maison, à l'école et dans sa collectivité; c'est un droit, un droit tout à fait fondamental. Lorsque des enfants commencent à s'enlever la vie et que les problèmes de santé mentale à l'échelle nationale atteignent un niveau record, nous, les adultes, devons réfléchir à la question et prendre des mesures. Nous espérons que vous partagerez cette vision.

Le président : Merci à tous. Nous allons commencer les questions en donnant la parole au sénateur Baker, vice-président du comité.

Le sénateur Baker : Merci à tous les témoins qui sont ici aujourd'hui. Les exposés étaient d'excellente qualité, et vos suggestions étaient aussi excellentes; je suis heureux que ces deux exposés figurent maintenant au compte rendu des travaux du comité du Sénat.

Je n'ai pas de question précise, mais j'aimerais peut-être vous demander, si vous le désirez, d'en dire un peu plus au sujet du deuxième point soulevé dans le dernier exposé, sous la rubrique « à quoi ressemblerait une stratégie nationale? » Vous avez dit qu'il faut réglementer les données des téléphones cellulaires pour les jeunes âgés de 12 ans ou moins car, avec des données complètes, un enfant d'aussi peu que 6 ans peut avoir accès, à partir d'un téléphone cellulaire, à tout ce qu'il veut en tout temps, sur Internet, souvent sans aucune frontière ni limite, et qu'il faut les protéger contre cela.

Voudriez-vous en dire un peu plus là-dessus? Vous n'êtes pas obligée de le faire, mais le voudriez-vous?

Mme Anderson : Tout à fait. Nous travaillons beaucoup avec des travailleurs de première ligne, avec des familles et des étudiants, avec des enseignants, et nous obtenons beaucoup d'informations directement des enseignants qui s'occupent des classes où des enfants âgés de six ans seulement se présentent en classe avec un iPhone, contenant toutes les données, et qui ont accès à tout ce qu'ils veulent, en tout temps. Les enfants n'ont pas la maturité sociale et émotionnelle nécessaires, à cet âge, pour savoir qu'on les incite à faire quelque chose, pour savoir qu'ils visitent un site qu'ils ne devraient pas visiter. Nous aimerions qu'il y ait à tout le moins une discussion sur la réglementation de ces choses, pour les enfants, parce que lorsque les parents achètent un forfait, c'est habituellement un forfait contenant certains types de textes et de données. Cela ne veut pas dire qu'ils ne pourront pas, à la maison, s'installer devant l'ordinateur, mais les ordinateurs sont plus gros, et il est à espérer qu'ils sont installés dans un endroit de la maison d'où les parents peuvent voir l'écran. Mais quand des enfants se promènent avec des appareils mobiles, nous estimons qu'il faudrait discuter de ce que nous pourrions faire pour aider à protéger nos enfants qui sont très jeunes contre les prédateurs ou les empêcher de se placer dans une situation dont ils ne pourront pas s'extirper.

Le sénateur Baker : Vous suggérez d'entamer un dialogue, de discuter de la façon dont nous pourrions approcher ce problème, comme vous l'avez dit, pour les enfants sous un certain âge.

Ms. Anderson: Right. If anybody has a teenager, they know that this is how they socialize. We don't believe in taking technology away from students at all, because this is their world and it's only going to grow bigger. But that doesn't mean that we can't take a look for our little ones to say they're driving at a certain age for a certain reason or they're able to drink at a certain age for a certain reason. We think it's a good dialogue to open up to ask what we are doing for technology for our little ones.

Senator Baker: Fahd, I wonder if I could ask you a general question? Do you find that people my age don't know anything about the Internet and perhaps we should be having greater discourse with people like yourself?

Mr. Alhattab: I would not say that you don't know anything about the Internet. That is not a claim that I will put my name to.

Senator Joyal: He knows a lot, believe me.

Mr. Alhattab: I think in some cases you know far more than we know. If you look at the biggest creators on the Internet, the people who make the most YouTube videos and post the most stuff, they're 16-year-olds. They're the ones who are creating the Internet. They're the ones who are not consuming. The older generation consumes. You go online, read the news and see the YouTube videos, but you don't post the YouTube videos. The young people are the ones who post.

I think we have a different perspective on where we are with the Internet and cybertechnology. A lot of that is consuming and creating. If we're able to have a discussion with youth around that and around where they see the Internet and where they fit in, it will change the way we look at legislation.

Senator McInnis: Thank you very much. This is very interesting. This is not my question, but Senator Jaffer could not be here today. She and I have been talking about working towards some mechanism that we can put in place with respect to a national strategy to bring together, coordinate and be more effective in getting it out to the public. I'm sure we'll want to talk about it. Her Human Rights Committee did a wonderful study a few years back on the subject. She would love to have been here to talk to you about this.

I want to talk about restorative justice because it's not the intent of this bill just to throw young people in jail. I want to get into it a bit because I remember back a number of years ago, when I practised law, restorative justice was just coming into vogue. Of course, you have the victim, and there's a victim impact statement, and the perpetrator is there and the family members and someone to oversee, a bit of an adjudicator and so on.

Mme Anderson : Exact. Ceux qui ont un adolescent savent que c'est ainsi que les ados socialisent. Nous ne croyons pas qu'il faut priver les étudiants de la technologie, pas du tout, parce qu'il est évident que cela fait partie de leur monde et que la technologie ne peut que prendre de plus en plus de place. Mais cela ne veut pas dire que nous ne pouvons pas réfléchir à la question, pour nos petits, leur dire qu'il y a des raisons de leur interdire de conduire avant un certain âge ou de boire avant un certain âge. Nous pensons qu'il serait bon d'avoir cette discussion et de réfléchir à ce que nous faisons, en matière de technologie, pour nos petits.

Le sénateur Baker : Fahd, pourrais-je vous poser une question d'ordre général? Pensez-vous que les gens de mon âge ignorent tout au sujet d'Internet et que nous devrions peut-être discuter davantage avec des gens comme vous?

M. Alhattab : Je ne dirais pas que vous ignorez tout à propos d'Internet. Je ne veux surtout pas qu'on pense que je suis d'accord avec une telle affirmation.

Le sénateur Joyal : Il est bien renseigné, croyez-moi.

M. Alhattab : Je crois que dans certains cas, vous en savez beaucoup plus que nous. Les gens qui créent le plus de contenu sur Internet, ceux qui produisent le plus grand nombre de vidéos sur YouTube et qui affichent le plus de choses, ce sont les jeunes de 16 ans. Ce sont eux qui créent Internet. Ce ne sont pas eux qui consomment. Ce sont les gens plus âgés qui consomment. Vous allez en ligne, vous lisez les nouvelles, vous regardez les vidéos sur YouTube, mais vous n'affichez pas de vidéos sur YouTube. Ce sont les jeunes qui en affichent.

Je crois que nous avons un point de vue différent sur notre situation par rapport à Internet et à la technologie virtuelle. Il y a beaucoup de consommation et de création. Si nous pouvions tenir une discussion avec des jeunes sur cette question et sur la façon dont ils voient Internet et leur place par rapport à Internet, cela changerait la façon dont nous envisageons la loi.

Le sénateur McInnis : Merci beaucoup. C'est très intéressant. Ce n'est pas ma question, mais la sénatrice Jaffer ne pouvait pas se présenter ici aujourd'hui. Elle et moi avons discuté de la mise en œuvre d'un mécanisme quelconque, lié à une stratégie nationale que nous pourrions élaborer et coordonner et présenter de manière plus efficace au public. Je suis certain que nous allons vouloir en parler. Son Comité des droits de la personne a réalisé il y a quelques années une magnifique étude sur ce sujet. Elle aurait adoré pouvoir être ici pour en discuter avec vous.

J'aimerais parler de la justice réparatrice, car le projet de loi n'a pas pour intention de jeter des jeunes en prison. J'aimerais en parler un peu plus, parce que je me souviens qu'il y a quelques années, lorsque je pratiquais le droit, la justice réparatrice commençait tout juste à être en vogue. Bien sûr, il y a la victime, il y a la déclaration de la victime, l'auteur du crime est présent ainsi que les membres de la famille et un superviseur, une sorte d'arbitre, et ainsi de suite.

The problem I saw at the end of the day was the follow-up. After everyone leaves the room, everyone is remorseful, they hug or whatever or shake hands, but it's the follow-up after. I want you to tell me: What is it that you do to keep in touch after? That has always been the problem. In one that I just participated in, no more than a year ago, the problem was follow-up, and then it was too late.

Rachel Gouin, Director, Research and Public Policy, Boys and Girls Clubs of Canada: I'd like to answer that, if I may. When those kinds of programs are delivered by a community organization like Boys and Girls Clubs, we have relationships with the youth already, and in many cases those are long-term relationships. We know them from a young age right through adulthood. We're better able to support them throughout that process and following to make sure they do what they said they were going to do and they're accompanied. The success rate has been 87 per cent. It's in our brief. Nearly 9 in 10 of the youth don't reoffend.

Our Kawartha Lakes Boys and Girls Club has such a program, and recently the Ontario Provincial Police has been referring cases of sexting, youth who have been caught who are between 12 and 17. This gives them a chance to make amends and fix the wrongs they've done.

I hear what you're saying. There's a real strength in working with community organizations that have a relationship with youth, to make sure it's not just a one time, we hug and everything is nice, that there's a follow-up.

Senator McInnis: How is the punishment doled out? What do you do? Is it education?

Ms. Gouin: It depends. From what I understand, the committee decides that together. It could be making reparations like an apology letter or an essay on the matter. It can be fundraising for a certain issue. It can be community service, but often it goes beyond just putting in a few hours in the community. Of course in some cases you could always volunteer with the Boys and Girls Clubs or put in hours with younger children or to educate around cyberbullying, for instance, with your younger peers.

Senator Joyal: Thank you for your presentation. You're most welcome. I have two sets of questions.

First, in your opinion, how many groups like yours are active at that level? I know one in Quebec is the Fondation Jasmin Roy. As a matter of fact, I support them directly. How many similar groups as yours might exist in Canada, and are you connected? In other words, are you exchanging initiatives, best practices,

Le problème que j'ai cerné, au bout du compte, concerne le suivi. Une fois qu'ils ont quitté la pièce, ils ont tout plein de remords, ils se prennent dans les bras ou se serrent la main, par exemple, mais il y a la question du suivi. J'aimerais que vous me disiez comment vous vous y prenez pour que ces gens restent en contact, après? Cela a toujours été le problème. J'ai participé tout récemment, il n'y a pas plus d'un an, à une de ces réunions, et le problème était le suivi, mais après, il était trop tard.

Rachel Gouin, directrice, Recherche et politiques publiques, Clubs Garçons et Filles du Canada : J'aimerais répondre à cette question, si vous me le permettez. Quand des organismes communautaires comme les Clubs Garçons et Filles mettent en œuvre ce type de programme, nous entretenons déjà des relations avec le jeune, et dans bien des cas, ce sont des relations de longue date. Nous les connaissons depuis qu'ils sont jeunes, jusqu'à ce qu'ils entrent dans l'âge adulte. Nous sommes mieux outillés pour les soutenir tout au long de ce processus et nous assurer qu'il y ait un suivi, qu'ils fassent ce qu'ils ont dit qu'ils feraient, et pour les accompagner. Le taux de réussite a atteint 87 p. 100. C'est indiqué dans notre mémoire. Près de 9 jeunes sur 10 ne commettent pas de nouvelle infraction.

Le Club Garçons et Filles de Kawartha Lakes propose un tel programme, et, récemment, la Police provinciale de l'Ontario nous a confié des jeunes coupables de sextage, des jeunes qui avaient été arrêtés alors qu'ils avaient entre 12 et 17 ans. Cela leur donne la possibilité de s'amender et de réparer les torts qu'ils ont causés.

Je comprends ce que vous dites. On gagne énormément à travailler avec des organismes communautaires qui ont établi des relations avec les jeunes, quand on veut s'assurer que cela ne se résume pas à une seule réunion, à l'issue de laquelle on se congratule, et qu'il y a un suivi.

Le sénateur McInnis : Et comment le châtiment est-il appliqué? Que faites-vous? S'agit-il d'éducation?

M. Gouin : Cela dépend. Selon ce que je comprends, ce sont les membres du comité qui prennent ensemble la décision. Le jeune pourrait devoir demander réparation, par exemple en écrivant une lettre d'excuses ou encore en rédigeant un essai sur la question. Il pourrait devoir participer à une campagne de financement pour une cause ou une autre. Il pourrait devoir faire des travaux communautaires, mais, souvent, on lui demande davantage que de consacrer quelques heures à sa collectivité. Bien sûr, dans certains cas, il pourrait faire du bénévolat auprès des Clubs Garçons et Filles ou travailler quelques heures auprès de jeunes enfants ou encore, par exemple, renseigner ses cadets au sujet de la cyberintimidation.

Le sénateur Joyal : Merci de votre exposé. Vous êtes la bienvenue. J'ai deux séries de questions.

Pour commencer, à votre avis, combien y a-t-il de groupes comme le vôtre qui travaillent dans ce domaine? Je sais qu'il y en a un au Québec, la Fondation Jasmin Roy. D'ailleurs, je soutiens directement cette fondation. Combien y a-t-il de groupes semblables au vôtre qui existent au Canada, les côtoyez-vous?

common objectives in terms of getting legislation amended, getting programs put into place at the provincial level and so forth?

Ms. Anderson: Yes, there are many groups that do great work. When Bessie and I started eight years ago, we had similar instances of our children being bullied, and we thought we would save the world at the school level and everything would be fine. However, the more you dig deep, you realize it's a huge issue, and we view it as a huge puzzle and there are many pieces to that puzzle. There are municipal changes, provincial changes and federal changes. There are lots of people out there doing great work.

It would be fantastic to have people across Canada coming together and sharing what they're doing because it is very piecemeal. People in Quebec are doing certain things, and people in different areas of Canada are doing other things. We do network with different people for sure; you have to.

Senator Joyal: There is no organization to try to group all of them and share best practices, initiatives and expertise.

Ms. Anderson: Correct me if I'm wrong because you guys are probably connected with many people, as we are. The Canadian Safe School Network and other organizations might hold seminars or workshops, but I don't think one large forum exists where everybody could get together and share best practices. That might be something to add to the national strategy.

Ms. Gouin: There is also PREVNet. There is a lot of sharing of resources and collaboration on certain issues. For example, the Boys and Girls Clubs of Canada has collaborated with the Canadian Mental Health Association to see how we can increase mental health support in communities for young children and youth. There are collaborations on issues like that.

Of course, a national strategy on bullying would help to rally all of us together to work more cohesively. We share resources, but we don't always have a guiding thread to our work. Boys and Girls Clubs has launched the Belonging campaign. It is the first Wednesday of May to try to shift the discussion from stopping bullying to restoring a sense of belonging and to promoting mental health in young people, which will help them have respectful relationships with one another.

We see that as the antidote. The education component is about letting young people know what the consequences of their actions are, and modelling the kind of behaviours and respect from each other is also very important.

Autrement dit, échangez-vous des initiatives ou des pratiques exemplaires, avez-vous des objectifs communs touchant les modifications de la loi, la mise en œuvre de programmes à l'échelon provincial, et ainsi de suite?

Mme Anderson : Oui, il existe de nombreux groupes qui font de l'excellent travail. Quand Bessie et moi-même avons commencé, il y a huit ans, c'est parce que nos enfants étaient victimes d'intimidation, et nous pensions pouvoir sauver le monde, à l'échelle de l'école, et que tout rentrerait dans l'ordre. Toutefois, plus vous creusez la question, plus vous réalisez que c'est un problème énorme, et nous voyons cela comme un énorme casse-tête qui compte de très nombreuses pièces. Il y a les changements à l'échelon municipal, à l'échelon provincial et à l'échelon fédéral. Il y a beaucoup de gens qui font de l'excellent travail.

Ce serait merveilleux que tous les intervenants du Canada se réunissent et discutent de ce qu'ils font, parce que c'est très fragmenté. Les gens du Québec font certaines choses, les gens de différentes régions du Canada font d'autres sortes de choses. Mais nous travaillons effectivement en réseau avec différentes personnes, évidemment, c'est inévitable.

Le sénateur Joyal : Il n'existe pas d'organisme qui regrouperait tous ces gens et mettrait en commun les pratiques exemplaires, les initiatives et l'expertise.

Mme Anderson : Corrigez-moi si je me trompe, mais vous êtes probablement en contact avec bien des gens, tout comme nous le sommes. Il y a des organismes comme le Canadian Safe School Network, par exemple, qui organisent parfois des conférences ou des ateliers, mais je ne crois pas qu'il existe un grand forum où tout le monde peut se réunir et discuter des pratiques exemplaires. Ce serait peut-être quelque chose à ajouter à une stratégie nationale.

Mme Gouin : Il y a aussi PREVNet. Il y a beaucoup d'échanges de ressources de collaboration, dans certains dossiers. Par exemple, les Clubs Garçons et Filles du Canada ont collaboré avec l'Association canadienne pour la santé mentale afin de trouver des moyens d'offrir un meilleur soutien en matière de santé mentale dans la collectivité pour les enfants et pour les jeunes. Il y a de la collaboration à l'égard d'enjeux de ce type.

Bien sûr, une stratégie nationale de lutte contre l'intimidation nous aiderait à regrouper nos forces et à travailler de façon plus cohérente. Nous partageons des ressources, mais notre travail ne profite pas toujours d'un fil conducteur. Les Clubs Garçons et Filles ont lancé la campagne Appartenance. Le premier mercredi du mois de mai, nous essayons de dévier du sujet de l'intimidation pour parler plutôt du rétablissement du sentiment d'appartenance et de la promotion de la santé mentale auprès des jeunes, dans le but de les aider à entretenir les uns avec les autres des relations fondées sur le respect.

Nous voyons cela comme un antidote. Le volet éducatif vise à renseigner les jeunes sur les conséquences de leurs actes, et il est également important de leur donner des modèles de comportement et d'attitudes respectueuses les uns envers les autres.

Senator Joyal: The other preoccupation I have is that the school environment has changed, but I don't want to say dramatically. The curricula at the provincial ministry of education should be part of the program to instruct the kids or teens on the impact of what they have in their hands.

I have young nephews who are four years old. They already spend hours and hours on their games. They are already islands unto themselves. School is where kids can socialize and meet other people daily, continuously — many people they don't know — and they have to adapt to an environment in which what they have in hand can be an arm and a tool at the same time. It seems that school curricula should have an aspect that teaches kids about the implications of that. A knife can be useful to cut meat, but it can be harmful when used without care against somebody.

There is a lack in the way the minister of education approaches the school environment today. It should be the first thing thought about because the first thing kids know in life these days is how to use their phone or their computer or other.

Did you make any representation at the provincial level as a group?

Ms. Anderson: We are certainly trying. The process is so slow and technology is so fast. Our school board, York Region District, is trying very hard to bring the social and emotional well-being of children in line with academic learning. Studies have been done on how important it is for children to belong and feel safe. Their academics will automatically improve because of that. Those are conversations we are trying to have. We are trying to talk to our local MPP also, with the colleges and universities having the Bachelor of Education program for teachers coming into their new careers so they have the skills, knowledge and experience.

We spoke to a student teacher just yesterday because it's Bullying Awareness Week in Ontario. They have not discussed bullying or youth mental health. Teachers wear many hats, but it would be great to send them into their new careers with sufficient skills to recognize what mental may look like in a 4-year-old or a 6-year-old, which may be different from a 16-year-old, and to recognize the signs of bullying and be able to answer those questions.

We are trying to have those conversations; we are constantly trying.

Le sénateur Joyal : L'autre problème qui me préoccupe, c'est que l'environnement des écoles a changé, même si je n'irais pas jusqu'à qualifier le changement de spectaculaire. Les programmes du ministère provincial de l'Éducation devraient passer par l'éducation des enfants et des adolescents sur les impacts de ce qu'ils ont entre les mains.

J'ai de jeunes neveux qui ont quatre ans. Ils passent déjà des heures et des heures à jouer à leurs jeux. Ils sont déjà, en soi, des îles. L'école, c'est l'endroit où les enfants peuvent socialiser et rencontrer d'autres personnes tous les jours, continuellement — de nombreuses personnes qu'ils ne connaissent pas —, et ils doivent s'adapter à un environnement dans lequel ce qu'ils ont entre les mains peut être une arme et un outil en même temps. Il me semble que le programme d'enseignement devrait avoir un volet où on enseigne aux enfants ce que cela suppose. Un couteau peut être utile pour couper de la viande, mais il peut être nuisible si on l'utilise sans faire attention, contre quelqu'un.

Il y a une lacune dans la façon dont le ministre de l'Éducation aborde le milieu scolaire aujourd'hui. Ce devrait être la première chose qui nous vient à l'esprit, puisque la première chose que les enfants apprennent dans la vie, de nos jours, c'est comment utiliser leur téléphone, leur ordinateur ou un autre appareil du genre.

Avez-vous formulé des observations à l'échelon provincial, en tant que groupe?

Mme Anderson : Nous tentons assurément de le faire. Le processus est si lent, et la technologie, si rapide. Notre conseil scolaire, celui du district de la région de York, déploie de très grands efforts pour que l'enseignement tienne compte du bien-être social et émotionnel des enfants. Des études ont été réalisées sur l'importance des sentiments d'appartenance et de sécurité pour les enfants. Leurs résultats scolaires s'amélioreront automatiquement grâce à ces sentiments. Ce sont des conversations que nous essayons de tenir. Nous tentons également de parler à nos députés provinciaux locaux et aux responsables des collèges et des universités qui offrent le programme de baccalauréat en éducation pour veiller à ce que les enseignants qui commencent leur nouvelle carrière possèdent les compétences, les connaissances et l'expérience nécessaires.

Pas plus tard qu'hier, nous avons parlé à un étudiant en enseignement parce que c'est la semaine de sensibilisation à l'intimidation en Ontario. Les étudiants n'ont pas discuté de l'intimidation ni de la santé mentale des jeunes. Les enseignants jouent de nombreux rôles, mais ce serait formidable de les envoyer dans leur nouvelle carrière munis de suffisamment de compétences pour reconnaître ce dont un problème de santé mentale pourrait avoir l'air lorsqu'il s'agit d'un enfant de 4 ou de 6 ans, qui pourrait être différent de celui d'un jeune de 16 ans, et pour reconnaître les signes de l'intimidation et être en mesure de répondre à ces questions.

Nous essayons de tenir ces conversations; nous essayons constamment.

Senator Joyal: What about at the college or secondary level?

The Chair: We will get back to you, Senator Joyal.

Senator Batters: I want to single out the emphasis you place on mental health — a very important issue to me, so I thank you for that.

I want to briefly touch on what Mr. Alhattab talked about and his desire to have enforcement measures age-appropriate in this bill and restorative justice taken into account. I draw to your attention that under this bill, for those who are of the appropriate age, the Youth Criminal Justice Act, as a governing force in this particular matter, has the provisions that would apply to the age-appropriateness and the restorative justice element. Many elements in there would apply to young people, so I wanted to draw that to your attention.

For the Bully Free Community Alliance, I appreciate your support of this bill. I thought you made an excellent point in your opening statement when you said:

> We understand the privacy concerns that surround Bill C-13. However, when our children, even adults, press an app or sign onto a social website, we have to ask the question: Do we really have privacy? The Criminal Code must be updated in order for law enforcement to response effectively and quickly when cybercrime occurs. Our society has changed, and our legislation needs to change with it.

That's really important to keep in mind. That's what we are trying to do with this bill, to keep up because our law has kind of fallen behind on this issue. Senator Jaffer, the Liberal critic of this bill, was discussing how her Human Rights Committee was studying this issue four years ago. Now, we're moving ahead with a bill.

Could you go a little further into the need for privacy and the need for action at the same time?

Ms. Anderson: I was listening to Senator Frum when she talked about being on the Internet and where our information is going. We're certainly not policy-makers or privacy commissioners. It's a little bit over our head sometimes because we don't know all of the other aspects. We come at it as parents of young children who need to manage that in our homes.

We've talked to Carol Todd and Glen Canning. We collaborate with the Canadian Centre for Abuse Awareness and work with the police. They all say that they need to be able to act quickly — take that information and do what we need to do to protect the child and stop it from happening. We wonder if only

Le sénateur Joyal : Qu'en est-il du niveau collégial ou secondaire?

Le président : Nous reviendrons à vous, sénateur Joyal.

La sénatrice Batters : Je veux souligner l'accent que vous mettez sur la santé mentale... C'est une question très importante pour moi, alors je vous en remercie.

Je veux aborder brièvement ce dont M. Alhattab a parlé ainsi que son désir de nous voir adapter les mesures d'application de la loi à l'âge dans ce projet de loi et veiller à ce que la justice réparatrice soit prise en compte. J'attire votre attention sur le fait que, aux termes du projet de loi, pour les personnes qui ont le bon âge, la Loi sur le système de justice pénale pour les adolescents, en tant que loi de premier plan dans ce domaine particulier, contient les dispositions qui s'appliqueraient aux éléments du caractère adapté à l'âge et de la justice réparatrice. Un grand nombre des éléments du projet de loi s'appliqueraient aux jeunes, alors je voulais porter ce fait à votre attention.

En ce qui concerne la Bully Free Community Alliance, je me réjouis de votre appui à l'égard de ce projet de loi. J'ai trouvé que vous aviez souligné un excellent point dans votre déclaration préliminaire, quand vous avez dit :

> Nous comprenons les préoccupations relatives à la vie privée en ce qui a trait au projet de loi C-13. Cependant, lorsque nos enfants, ou même des adultes, utilisent une application ou s'inscrivent sur un site social en ligne, nous devons nous poser la question suivante : avons-nous vraiment une vie privée? Le Code criminel doit être mis à jour si l'on veut que les forces de l'ordre puissent réagir efficacement et rapidement à la cybercriminalité. Notre société a changé, et il faut que nos lois changent en même temps.

Il est vraiment important de ne pas l'oublier. C'est ce que nous tentons de faire grâce à ce projet de loi : nous tenir à jour parce que nos lois ont en quelque sorte pris du retard à cet égard. La sénatrice Jaffer, critique libérale de ce projet de loi, a abordé le fait que son Comité des droits de la personne avait étudié cette question il y a quatre ans. Maintenant, nous allons de l'avant avec un projet de loi.

Pourriez-vous nous donner plus de détails sur le besoin de protéger la vie privée tout en prenant des mesures?

Mme Anderson : J'écoutais la sénatrice Frum quand elle a parlé de la présence sur Internet et de ce qui arrive à nos renseignements. Nous ne sommes certainement pas des décideurs ni des commissaires à la protection de la vie privée. Nous sommes parfois un peu dépassés parce que nous ne connaissons pas tous les autres aspects. Nous nous y attaquons en tant que parents de jeunes enfants qui ont besoin de gérer cela dans nos foyers.

Nous avons parlé à Carol Todd et à Glen Canning. Nous collaborons avec le Centre canadien de sensibilisation aux abus, et nous travaillons avec la police. Ils disent tous qu'ils doivent pouvoir agir rapidement... Prendre ces renseignements et faire ce qu'il faut pour protéger l'enfant et empêcher l'intimidation. Nous

they had had that legislation earlier — coulda, shoulda, woulda — but let's move forward. We're all concerned about our privacy. I am concerned when I'm online too, but I don't know where to find that balance. I know only that when we talk to the parents and see what happens to these children, we know there has to be something we can do; and this seems to be the great first step forward.

Senator Batters: Because you brought up her name, Carol Todd, we spoke briefly about her yesterday with Mr. Geist. I was asking him about a particular CBC interview that she had done. We didn't have the transcript at the time but I have it today. I want to pass along her comment because she kind of clarified her comments she made at the House of Commons committee. In that transcript, Carol Todd said, "I think it needs to be passed soon. It needed to be passed many years ago, in my eyes, as soon as technology started to show its ugly head." She went on to say, "You know I did talk about splitting" — meaning the bill — "and in my personal views, I don't know why we can't split, but it was explained to me that it couldn't be split for the reasons that you have the cyberbullying and cyber harassment clauses, and then you have the other clauses that have to do with investigative powers, searching and online looking into the stuff. It was shared with me that they have to be hand in hand." And, that was the end of her quote on that particular portion. I think that's very important to keep in mind.

You, today, have the ability, as you're in front of a Senate of Canada committee, to relay to Canadians the important work that you do with your particular organization. For the two of you that are here from the Bully Free Community Alliance, for someone who might be watching this committee hearing or will read this transcript, what good, practical advice would you give to a young Canadian, or that youth's parents, who might be the subject of cyberbullying right now?

Ms. Anderson: Thank you for the opportunity. We try to keep it simple. Number one is just to remove all technology from the bedroom at night. Nothing good happens in the middle of the night when you're trying to respond. Kids will get up in the middle of the night when their phone buzzes. Even if it's bad, they want to know what people are saying. They value what some kid they don't know at another school is saying about them.

We have to pay attention to that. So, having all technology — iPads, iPods, cellphones — out of the bedroom at night.

There have been studies done that kids are losing sleep, and they are going to school not well rested. It becomes a vicious circle. So that would be one.

nous demandons ce qui serait arrivé si seulement on avait eu cette mesure législative plus tôt — si on avait su, il aurait fallu, on aurait dû —, mais regardons en avant. Nous nous préoccupons tous de notre vie privée. Je suis inquiète, moi aussi, lorsque je suis en ligne, mais je ne sais où trouver cet équilibre. Je sais seulement que, quand nous parlons aux parents et que nous voyons ce qui arrive à ces enfants, nous savons qu'il y a sûrement quelque chose que nous pouvons faire, et cela semble être le premier grand pas en avant.

La sénatrice Batters : Puisque vous avez mentionné Carol Todd, je dois vous dire que nous avons brièvement parlé d'elle, hier, avec M. Geist. Je lui posais des questions au sujet d'une entrevue particulière qu'elle avait accordée à la CBC. Nous n'avions pas la transcription à ce moment-là, mais je l'ai aujourd'hui. Je veux transmettre son commentaire parce qu'elle a un peu clarifié les observations qu'elle avait faites devant le comité de la Chambre des communes. Dans cette transcription, on peut dire que Carol Todd a dit : « Je pense qu'il faut l'adopter bientôt. Il fallait l'adopter il y a de nombreuses années, à mon avis, dès que la technologie a commencé à se profiler à l'horizon. » Elle a poursuivi en disant : « Vous savez que je n'ai pas parlé de le scinder » — en parlant du projet de loi — « et je ne vois pas, personnellement, pourquoi nous ne pouvons le scinder, mais on m'a expliqué qu'il ne pouvait pas être scindé parce qu'il contient des dispositions relatives à la cyberintimidation et au cyberharcèlement, de même que les autres dispositions qui concernent les pouvoirs d'enquête, les perquisitions et les recherches en ligne sur les choses. On m'a affirmé que ces dispositions sont indissociables. » Et c'est la fin de sa déclaration sur cet aspect particulier. Je pense qu'il est très important de ne pas l'oublier.

Vous avez aujourd'hui la capacité, puisque vous êtes devant un comité du Sénat du Canada, de transmettre aux Canadiens le travail important que vous faites au sein de votre organisation particulière. Je m'adresse aux deux représentantes de la Bully Free Community Alliance qui sont ici : pour une personne qui pourrait être en train de regarder la séance du comité ou qui en lira la transcription, quels bons conseils pratiques donneriez-vous à un jeune Canadien — ou aux parents de ce jeune — qui serait victime de cyberintimidation actuellement?

Mme Anderson : Merci pour l'occasion. Nous tentons de rester dans la simplicité. La première étape consiste tout simplement à retirer toute la technologie de la chambre à coucher, le soir. Il n'arrive rien de bon en pleine nuit, lorsqu'on tente d'intervenir. Les jeunes vont se lever au beau milieu de la nuit quand leur téléphone sonne. Même si c'est mal, ils veulent savoir ce que les gens disent. Ils accordent de la valeur à ce qu'un jeune qu'ils ne connaissent pas, qui fréquente une autre école, dit à leur sujet.

Nous devons prêter attention à cela. Ainsi, retirer toute la technologie — les iPad, les iPod, les téléphones cellulaires — de la chambre à coucher la nuit.

Des études ont démontré que les jeunes manquent de sommeil et qu'ils ne sont pas bien reposés quand ils vont à l'école. Cela devient un cercle vicieux. Donc, ce serait une mesure à prendre.

Have that open communication. You do pay for the cellphone, and they're still a minor. You discuss the responsibilities that go along with having that hand-held device. You know what? The kids don't like it, but it's our responsibility to look after them, and you can word it in that way, that you are doing your job as a parent, that you have to make sure things are safe and that you're not spying on them. You just need to know that things are safe.

Senator Batters: I agree.

Senator McIntyre: Thank you all for your presentations.

First of all, I note that the Boys and Girls Clubs favours a restorative justice approach in all but the most severe cases. I am pleased to hear that.

Ms. Anderson and Ms. Schinas-Vlasis, the mental health issue has been raised. I noted you also raised it in your memo, which was given to us. As a matter of fact, you mention that as your organization developed, your main concerns were technology and mental health.

Now, my question is this: Could you elaborate further on the relationship between bullying and cyberbullying and mental health issues? In other words, do a lot of the young people involved in bullying or cyberbullying, either as victims or aggressors, suffer from mental health issues? As Senator McInnis rightly pointed out, is there a follow-up? If there is a follow-up, what kind do we have? Do we have a follow-up with the community mental health centres in the area? Could you elaborate on that, please?

Ms. Anderson: Well, youth mental health is an epidemic. It's a tough question because just because somebody is bullied, it doesn't mean they're going to end up with mental health issues, or just because a child bullies, it doesn't mean that they do have a mental health issue. However, we do have children who are much more resilient than others. Something could be said to them and it rolls right off their shoulders. For others, it percolates in them. Depending on the ongoing harassment or on the ongoing images that might be circulating, it can literally change their brain and have lifelong implications.

What can we do to help that? We need to start very early. A lot of money has been given to post-secondary education on mental health, which is excellent. This is because we have students leaving university before December, because they can't manage. But we really need to focus on the little ones, as well, to make sure that we catch it early on and can help guide them through that social and emotional aspect of school.

Ayez cette communication ouverte. Vous payez pour le téléphone cellulaire, et l'enfant est encore mineur. Vous discutez des responsabilités associées au fait de posséder cet appareil portatif. Vous savez quoi? Les jeunes n'aiment pas cela, mais nous devons nous occuper d'eux, et vous pouvez le formuler de cette manière : vous faites votre travail de parent, et vous vous assurez seulement que l'enfant est en sécurité et vous ne l'espionnez pas. Vous devez seulement savoir que la situation est sécuritaire.

La sénatrice Batters : Je suis d'accord.

Le sénateur McIntyre : Je vous remercie tous de vos exposés.

Tout d'abord, je remarque que les Clubs Garçons et Filles sont favorables à une approche axée sur la justice réparatrice dans tous les cas, sauf les plus graves, Je suis heureux de l'entendre.

Mesdames Anderson et Schinas-Vlasis, la question de la santé mentale a été soulevée. J'ai remarqué que vous l'aviez également soulignée dans votre exposé, qui nous a été remis. D'ailleurs, vous mentionnez que, au fil de l'évolution de votre organisation, vos principales préoccupations sont devenues la technologie et la santé mentale.

Or, ma question est la suivante : pourriez-vous nous décrire plus en détail le lien entre l'intimidation, la cyberintimidation et les problèmes de santé mentale? Autrement dit, les jeunes qui sont impliqués dans l'intimidation ou la cyberintimidation, en tant que victimes ou agresseurs, sont-ils nombreux à avoir des problèmes de santé mentale? Comme l'a demandé avec raison le sénateur McInnis, y a-t-il un suivi? Le cas échéant, de quel genre s'agit-il? Faisons-nous un suivi auprès des centres de santé mentale communautaires de la région? Pourriez-vous en dire plus à ce sujet, s'il vous plaît?

Mme Anderson : Eh bien, les problèmes de santé mentale sont épidémiques chez les jeunes. Il est difficile de répondre à cette question, car le simple fait qu'une personne est victime d'intimidation ne signifie pas qu'elle va finir par avoir des problèmes de santé mentale, et le simple fait qu'un enfant en intimide un autre ne signifie pas qu'il a un problème de santé mentale. Cependant, certains enfants sont beaucoup plus résilients que d'autres. On peut leur dire quelque chose, et cela les laissera tout à fait indifférents. Pour d'autres, cela va les toucher profondément. Selon qu'il s'agira de harcèlement constant ou d'images qui pourraient circuler continuellement, l'intimidation peut littéralement changer leur cerveau et avoir des répercussions à vie.

Alors, qu'est-ce qu'on peut faire? Nous devons commencer très tôt. Beaucoup d'argent a été affecté à l'éducation post-secondaire en santé mentale, ce qui est excellent. C'est parce que certains étudiants abandonnent l'université avant décembre parce qu'ils n'arrivent pas à gérer la situation. Mais, en réalité, nous devons nous concentrer sur les tous petits également, pour nous assurer que nous pouvons reconnaître le problème tôt et orienter les enfants dans cet aspect social et émotionnel de l'école.

Ms. Schinas-Vlasis: Being proactive is key. We find that when we are speaking with children, especially with the younger children, it's as simple as teaching children how to be a good friend. When they can grasp that and understand what being a good friend means, it leads later on to kindness. It's just all about being proactive and teaching children about being good and having empathy. These are all traits that they need to learn at a young age, and then we have fewer problems later on.

Ms. Anderson: Because when they communicate on line, they can't see a face. They can't see that somebody is hurt.

Senator McIntyre: I understand what you're saying, but is there a follow-up with community mental health centres, is what I'm driving at? Because those centres play a major role in helping those kids with mental health issues.

Ms. Schinas-Vlasis: Absolutely, and we're finding that the lineups and wait times are getting longer and longer. Just to get in to be seen, the wait time is long. The follow-up is not happening as much because of the long wait times. We would like to see that changed because if children are at a crisis point, then there should be a lot of follow-up. They should be getting the supports that they need right away.

Ms. Anderson: We have a crisis centre at our local hospital, and they take the person who tried to take their own life, as opposed to the person who has been talking about it. They're both crisis situations, but they're strapped as well. People's insurance runs out, and then they're left with monetarily not being able to afford care for their children.

[*Translation*]

Senator Dagenais: Thank you for your presentations. Let me congratulate you on your work. I think your mission and the values that you are promoting fall under what used to be called training, prevention and education for youth.

New technologies can have devastating effects. Sometimes, we can do great things with them, but they can also wreak havoc. In fact, new technologies can often lead young people down a slippery slope.

I think the government has good reason to be concerned and to want to provide police officers with the tools they need to do their jobs better. Could you elaborate on the balance needed between effectively applying the legislation and what we talked about earlier in terms of human rights?

Ms. Gouin: One right is not better than another. People have a right to protection against violence and harassment, but they also have a right to the protection of their privacy.

Mme Schinas-Vlasis : La proactivité est cruciale. Lorsque nous parlons avec les enfants, surtout avec les plus jeunes, nous constatons que c'est aussi simple que de leur montrer comment être un bon ami. Une fois qu'ils peuvent saisir cette notion et comprendre ce que suppose le fait d'être un bon ami, cela mène, plus tard, à la gentillesse. Il s'agit tout simplement d'être proactif et d'enseigner aux enfants à être bons et à faire preuve d'empathie. Ce sont tous des traits qu'ils doivent apprendre à un jeune âge, et nous avons moins de problèmes par la suite.

Mme Anderson : Parce que, lorsqu'ils communiquent en ligne, ils ne peuvent pas voir le visage de leur interlocuteur. Ils ne peuvent pas voir que quelqu'un est blessé.

Le sénateur McIntyre : Je comprends ce que vous dites, mais y a-t-il un suivi auprès des centres de santé mentale communautaires? C'est à cela que je veux en venir, parce que ces centres jouent un rôle majeur pour ce qui est d'aider ces enfants à régler leurs problèmes de santé mentale.

Mme Schinas-Vlasis : Absolument, et nous constatons que les files d'attente et les temps d'attente ne cessent de s'allonger. Ne serait-ce que pour être admis et obtenir une consultation, le temps d'attente est long. Il n'y a pas autant de suivi en raison des longs temps d'attente. Nous voudrions que cette situation change, car si les enfants sont en crise, il devrait y avoir beaucoup de suivi. Ils devraient obtenir immédiatement le soutien dont ils ont besoin.

Mme Anderson : À notre hôpital local, nous avons un centre de crise, où on admet la personne qui a tenté de s'enlever la vie plutôt que celle qui parle de le faire. Ce sont deux situations de crise, mais on est également à court d'argent. La police d'assurance des gens arrive à échéance, et ils se retrouvent dans une situation financière où ils n'ont pas les moyens de prendre soin de leurs enfants.

[*Français*]

Le sénateur Dagenais : Merci pour vos présentations. Je veux vous féliciter pour votre travail. Votre mission et les valeurs que vous véhiculez font partie, je pense, de ce qu'on appelait précédemment la formation, la prévention et la sensibilisation auprès des jeunes.

Les nouvelles technologies peuvent être dévastatrices. Parfois, on peut faire de grandes choses, mais elles peuvent être aussi très dévastatrices. D'ailleurs, souvent, ce sont les nouvelles technologies qui peuvent entraîner les jeunes sur des pentes savonneuses.

Je pense que le gouvernement a raison de s'inquiéter et de veiller à donner des outils aux policiers pour leur permettre de mieux faire leur travail. J'aimerais vous entendre parler de la préservation de l'équilibre entre l'application efficace de la loi et ce dont on a parlé précédemment, soit les droits de la personne.

Mme Gouin : Il n'y a pas un droit qui va au-delà de l'autre. Les gens ont droit à la protection contre la violence et contre le harcèlement, mais ils ont aussi droit à la protection de leur vie privée.

Young people are entitled to all those rights equally. We need a balance, but we cannot set one right against another. I trust you with that, with the help of experts in the field.

What we care about is ensuring that young people can fully enjoy all their rights: the right to the security of their person, the right to privacy, and so on. We trust the experts who were here. We are pleased to see that there are a number of different voices speaking to this issue, and we are counting on you to make wise choices. In the meantime, we will continue to support young people.

[*English*]

Senator Plett: I want to follow up a little bit on the answer you gave Senator Batters about having no devices in the bedroom in the evening. As a parent and now a grandparent, I would certainly endorse that.

However, we deal with legislation here all the time, and I'm dealing with a particular piece of legislation right now where parents are telling me that their three-, four- and five-year-old children are old enough to make decisions. How do you square that box, when a parent says a five-year-old or a three-year-old is old enough to make a life-changing decision, and they take these devices into the bedroom? Who do we need to educate, the kids or the parents? How do we educate the parents? That would be my first question. I have one for the other panel.

Ms. Anderson: If we had the perfect answer, that would be fantastic. We struggle with it at schools because the devices are in the classroom to be used as an educational tool. Pictures are taken, and nobody passes notes anymore. They make rude comments about somebody else. The actual cyberbullying is going on in the classroom as the teacher is trying to teach.

We have said to the principals, "Maybe you want to have cellphones used only when the teacher says it's time to pull your cellphone out and look on the Internet or the Moodle for some particular topic or instruction." However, a lot of the principals won't do it because parents will say, "I want to be able to get ahold of my child at any time of the day at any point."

Senator Plett: Exactly.

Ms. Anderson: We had one principal say to a parent, "Well, use the office phone. If you want to call and speak to your child, we will bring them down and you can speak to them on the phone."

Les jeunes ont droit à tous ces droits de façon égale. Il faut trouver l'équilibre, mais on ne peut opposer un droit à un autre. Je vous fais confiance, à cet égard, avec l'aide des experts dans ce domaine.

Ce qui nous préoccupe, c'est que les jeunes puissent profiter pleinement de tous leurs droits : le droit à la sécurité de leur personne, le droit à la vie privée, et cetera. On fait confiance aux experts qui étaient ici. On est heureux de voir qu'il y a plusieurs différentes voix qui s'expriment à ce sujet, et on compte sur vous pour faire des choix judicieux. De notre côté, nous allons nous assurer de continuer à appuyer les jeunes.

[*Traduction*]

Le sénateur Plett : Je veux revenir un peu à la réponse que vous avez donnée à la sénatrice Batters au sujet du retrait des appareils de la chambre à coucher, le soir. En tant que parent et, maintenant, que grand-parent, je serais certainement favorable à cette mesure.

Toutefois, nous traitons tout le temps de lois ici, et je suis actuellement en train d'étudier un projet de loi particulier dans un contexte où des parents me disent que leur enfant de trois, quatre ou cinq ans est assez grand pour prendre des décisions. Comment peut-on régler ce problème, quand un parent dit qu'un enfant de cinq ans ou de trois ans est assez vieux pour prendre une décision cruciale et le laisse conserver cet appareil dans sa chambre à coucher? Qui devons-nous sensibiliser : les enfants ou les parents? Comment pouvons-nous sensibiliser les parents? Ce serait ma première question. J'en ai une autre pour l'autre groupe.

Mme Anderson : Si j'avais la réponse parfaite, ce serait fantastique. Nous luttons contre ce problème dans les écoles parce que les appareils sont utilisés dans la salle de classe comme outils pédagogiques. On prend des photographies, et plus personne ne se passe des messages sur de petits bouts de papier. On formule des commentaires irrespectueux au sujet de quelqu'un d'autre. La cyberintimidation en tant que telle a lieu dans la salle de classe, pendant que l'enseignant essaie d'enseigner.

Nous avons dit aux directeurs : « Vous voulez peut-être que les téléphones cellulaires ne soient utilisés que lorsque l'enseignant dit que c'est le moment de sortir son téléphone cellulaire pour faire une recherche sur Internet ou dans le Moodle sur un sujet ou un apprentissage particulier. » Cependant, beaucoup de directeurs ne veulent pas le faire parce que les parents vont dire : « Je veux être capable de joindre mon enfant à tout moment de la journée, n'importe quand. »

Le sénateur Plett : Exactement.

Mme Anderson : Un de nos directeurs a dit à un parent : « Eh bien, utilisez le téléphone du bureau. Si vous voulez téléphoner et parler à votre enfant, nous allons le faire descendre, et vous pourrez lui parler au téléphone. »

There is education for everybody. I hate to put the onus on just the kids, like it's their responsibility, because it's all our responsibility. Parents absolutely need to be educated. A five-year-old making a decision on where they go on the Internet is not good.

Senator Plett: It's unacceptable.

Ms. Schinas-Vlasis: We liken it a lot to whether you would give your 12-year-old your car keys and say, "Honey, go down to the corner store and pick up some milk." You wouldn't because, at 12, they don't know how to drive a car. It's the same idea when you're handing a cellphone to someone who is under 12 and you have no instruction or no guidelines. They could potentially cause damage to themselves or others.

Senator Plett: I agree. However, there is one difference here. The 12-year-old probably knows how to use the computer and Internet much better than the parent does.

Ms. Anderson: They can get anywhere they want to go. That's for sure.

Senator Plett: Fair enough. I know there's no perfect answer.

Ms. Anderson: It's important to have these discussions, 100 per cent.

Senator Plett: For the Boys and Girls Clubs, just further to this particular answer, do you have programs that would really teach these kids that there are much more constructive activities that they can get involved in? Of course you only have them maybe one night out of the week, but certainly when kids are so tired that they just want to go to bed when they come home, they maybe won't be on the iPad. What do you do to maybe tire the kids out enough that maybe they want to stay away from it?

Mr. Alhattab: I make them run laps around the gym over and over again. We definitely have tons of programs at our Boys and Girls Club. A lot of the youth and kids who come to our Boys and Girls Clubs are there multiple times a week, which is fantastic. Parents love us because, yes, they do go home tired. They get their energy out.

We do also run a lot of computer technology programs. We have had media literacy programs where they're learning to make videos and how to use Photoshop. They're learning to use the tools on the computer for effective things and for fun things that can be used, so it's showing how the computer and the Internet can be used for very productive things.

Il y a de la sensibilisation à faire auprès de tout le monde. Je déteste mettre le fardeau sur les enfants seulement, comme si c'était leur responsabilité, parce que c'est notre responsabilité à tous. Les parents doivent absolument être sensibilisés. Un enfant de cinq ans qui décide où il va sur Internet, ce n'est pas une bonne chose.

Le sénateur Plett : C'est inacceptable.

Mme Schinas-Vlasis : Une analogie que nous utilisons beaucoup, c'est de comparer à une situation où vous remettez vos clés de voiture à votre enfant de 12 ans pour ensuite lui dire : « Chéri, va chercher du lait au dépanneur. » Vous ne le feriez pas parce qu'à 12 ans, on ne sait pas comment conduire une voiture. C'est la même idée lorsqu'on donne un téléphone cellulaire à quelqu'un qui a moins de 12 ans sans lui donner de directives ou de lignes directrices. Il pourrait se causer du tort à lui-même ou en causer à d'autres.

Le sénateur Plett : Je suis d'accord. Toutefois, il y a une différence. L'enfant de 12 ans sait probablement comment utiliser l'ordinateur et Internet, beaucoup mieux que le parent.

Mme Anderson : Il peut se rendre où il veut. C'est certain.

Le sénateur Plett : Très bien. Je sais qu'il n'y a pas de réponse parfaite.

Mme Anderson : Il est important de tenir ces discussions, absolument.

Le sénateur Plett : Je m'adresse aux Clubs Garçons et Filles; je veux seulement approfondir cette réponse particulière : avez-vous des programmes qui permettraient vraiment d'enseigner à ces enfants qu'il y a des activités beaucoup plus constructives auxquelles ils peuvent s'adonner? Bien entendu, vous ne les avez peut-être qu'un soir la fin de semaine, mais, certainement, lorsque les enfants sont si fatigués qu'ils veulent seulement aller au lit quand ils rentrent à la maison, ils ne seront peut-être pas sur l'iPad. Que peut-on faire peut-être, pour que les enfants soient tellement fatigués qu'ils voudront peut-être s'abstenir de l'utiliser?

M. Alhattab : Je leur fais faire le tour du gymnase à la course, encore et encore. Nous avons assurément des tonnes de programmes à nos Clubs Garçons et Filles. Beaucoup des jeunes et des enfants qui viennent à nos clubs sont là plusieurs fois par semaine, ce qui est formidable. Les parents nous adorent parce que, oui, les jeunes rentrent bel et bien fatigués à la maison. Ils dépensent leur énergie.

Nous offrons également beaucoup de programmes d'informatique. Nous avons eu des programmes de médiatique, où les jeunes apprennent à faire des vidéos et à utiliser Photoshop. Ils apprennent à se servir des outils informatiques pour des choses efficaces et pour des choses amusantes qui peuvent être utilisées; nous leur montrons donc comment l'ordinateur et Internet peuvent être utilisés pour des choses très productives.

We have tonnes of programs around sports, leadership programs and arts programs that allow them to create friends in their local community and around their neighbourhood and kind of use their time away from the cellphone. A lot of the clubs discourage the use of cellphones while they're in our program. They say, "You can use it at a different time. We're playing basketball. You can' really text when you're playing basketball." Or, "We're doing a leadership program. As a young leader, you have to focus your attention on what is happening now, right?" So we discourage the use of that so that we have their attention and we're teaching them the positive values of being good citizens and being good friends and creating those relationships.

Senator Plett: At many meetings, we have to check our cellphones at the door when we walk in.

The Chair: I have a question for the alliance representatives. Earlier today, we had a representative from the Canadian Bar Association appear, and one of their concerns about the legislation was they suggested the recklessness standard with respect to the criminal intent element of the bill be removed. I have some personal concerns about that. The justice ministry definition of "recklessness" as it applies to this legislation captures those who recognize that there is a risk the person did not consent but proceeded to share the image anyway.

My concern is that we're suggesting these people should be free and clear, essentially, if they distribute such an image if there is no clear knowledge of the circumstances to determine if the person depicted had consented. In my view, it greatly reduces the effectiveness of the legislation. I wonder if you've taken a look at that issue. I know the bar apparently was concerned about overreach, but we still have significant police and Crown discretion. Ultimately the judge is going to make a determination as well. I wonder if you have a comment on that.

Ms. Anderson: We haven't read the entire legislation from beginning to end. A little bit of it is over our head. I'm not going to lie. We're here as parents and community members. But having this bill and youth and parents in our society knowing that there is a crime involved when you distribute those images is going to make people stop and think before doing it. That is our feeling as parents. Being able to have that discussion as kids, even when they are getting their cellphone for the first time, saying, "Here is your responsibility, but please understand that there is now legislation and law that's attached to the cellphone. So think twice about what you say and what you send, as simple as that."

Nous offrons des tonnes de programmes sportifs, des programmes de leadership et des programmes artistiques qui leur permettent de nouer des amitiés dans leur communauté locale et dans leur quartier, ainsi que de passer du temps loin du téléphone cellulaire. Bien des clubs découragent l'utilisation des téléphones cellulaires pendant que les jeunes participent à notre programme. On leur dit : « Vous pouvez l'utiliser à d'autres moments. Là, nous jouons au basketball. Tu ne peux pas vraiment envoyer des messages textes pendant que tu joues au basketball. » Ou : « Nous participons à un programme de leadership. En tant que jeune leader, tu dois fixer ton attention sur ce qui se passe maintenant, n'est-ce pas? » Nous décourageons donc l'utilisation de cet appareil afin d'avoir toute leur attention et de leur enseigner les valeurs positives associées au fait d'être de bons citoyens et d'être de bons amis ainsi qu'à la création de ces relations.

Le sénateur Plett : À de nombreuses réunions, nous devons laisser nos téléphones cellulaires à la porte avant d'entrer.

Le président : J'ai une question pour les représentants de l'alliance. Plus tôt, aujourd'hui, nous avons accueilli un représentant de l'Association du Barreau canadien, et l'une de ses préoccupations au sujet du projet de loi a amené l'ABC à proposer le retrait de la norme d'insouciance relative à l'élément de l'intention criminelle du projet de loi. Personnellement, j'ai quelques préoccupations à cet égard. Selon le ministère de la Justice, la définition du terme « insouciance », au sens du projet de loi, englobe les personnes qui reconnaissent qu'il y avait un risque que la personne n'ait pas été consentante, mais qui ont tout de même diffusé l'image.

Je crains que nous donnions à penser que ces personnes devraient être dégagées de toute responsabilité, essentiellement, si elles distribuent une telle image et qu'elle n'était pas clairement consciente de la situation pour déterminer si la personne figurant sur l'image avait consenti à sa distribution. À mon avis, cela réduit grandement l'efficacité du projet de loi. Je me demande si vous vous êtes penchés sur cette question. Je sais que le Barreau semblait craindre qu'on aille trop loin, mais nous avons encore d'importants pouvoirs discrétionnaires pour la police et la Couronne. Au bout du compte, le juge va rendre une décision, lui aussi. Je me demande si vous avez un commentaire à formuler à ce sujet.

Mme Anderson : Nous n'avons pas lu le projet de loi en entier, du début à la fin. Nous sommes un peu dépassés par certains passages. Je ne vais pas mentir. Nous sommes ici en tant que parents et membres de la collectivité. Mais le fait que ce projet de loi existe et que les jeunes et les parents dans notre société sachent que la distribution de ces images constitue un acte criminel fera que les gens y penseront à deux fois avant de le faire. C'est notre impression, en tant que parents. Nous avons l'occasion d'avoir cette discussion lorsqu'ils sont encore petits, même au moment où ils reçoivent leur premier téléphone cellulaire, de leur dire : « Voici ta responsabilité, mais comprends bien qu'il y a maintenant une loi et que tu dois respecter la loi lorsque tu

You can pick apart every piece of the legislation, and the privacy aspect is big, but we are heading into waters that we haven't been through before. I guess that would be my answer. I think it's really important because kids need to know that there is a crime attached. We don't want them to go to jail, every single person who distributes something, but they need to know it's there.

The Chair: I read that as your support of the recklessness inclusion in the legislation.

Ms. Anderson: Yes.

[*Translation*]

Senator Boisvenu: I find your comments very relevant. If you allow an eight-, nine-, or ten-year-old to have a tool like that and spend all night in his or her bedroom, you might as well give the key to the child's room to a stranger or a pedophile.

In my view, no piece of legislation will replace the vigilance of parents. Pedophiles are able to contact children because they know the parents are not there.

As such, I think police officers should be given special powers, powers that go beyond the current framework of the Criminal Code. We are now dealing with people who use technology and tools to be in contact with our children, which the Criminal Code historically has never foreseen.

I see people objecting just based on the principle of protecting privacy. I do not know whether you heard their testimony. Do you feel that we are putting the criminals' right to privacy before the children's right to protection?

[*English*]

Ms. Schinas-Vlasis: Yes. Very short answer: Yes.

Senator Baker: I have just one question to the Boys and Girls Club. When you appeared before the House of Commons committee, you recommended splitting the bill. From your presentation before the Senate committee now, you appear to not be suggesting that but saying very strongly, yes, protect children and youth from cyberbullying, but you must also protect their right to privacy. And you are suggesting not a split of the bill, but that we pay particular attention to the Privacy Commissioner and their recommendations. Am I correct in that? Could you elaborate on that?

utilises ton téléphone cellulaire. Par conséquent, réfléchis à deux fois à ce que tu dis et à ce que tu envoies; c'est aussi simple que cela. »

On peut décortiquer toutes les mesures du projet de loi, et l'aspect lié à la protection de la vie privée est énorme, mais nous nous dirigeons vers des zones encore inexplorées. Je suppose que ce serait ma réponse. Je pense que c'est vraiment important, parce que les enfants doivent savoir qu'un crime y est associé. Nous ne voulons pas qu'ils aillent en prison — chacune des personnes qui distribuent quelque chose —, mais elles doivent savoir que ce crime existe.

Le président : J'interprète cela comme un appui de votre part en ce qui concerne l'inclusion dans le projet de loi de la disposition relative à l'insouciance.

Mme Anderson : Oui.

[*Français*]

Le sénateur Boisvenu : Vos commentaires m'apparaissent très pertinents. Lorsqu'on donne un outil de cette nature à un enfant de huit, neuf ou dix ans, et qu'on lui permet de l'avoir toute la nuit dans sa chambre à coucher, c'est comme si on donnait la clé de sa chambre à un étranger ou à un pédophile.

À mon avis, aucune loi ne remplacera la vigilance des parents. Lorsqu'un pédophile peut entrer en contact avec un enfant, c'est parce qu'il sait que les parents sont absents.

Dans ce cadre, je crois qu'il faut donner des pouvoirs spéciaux aux policiers, des pouvoirs qui dépassent le cadre actuel du Code criminel, parce qu'on fait affaire à des gens qui utilisent des technologies, des moyens pour entrer en contact avec nos enfants, que le Code criminel n'a jamais prévus, historiquement.

Je vois des gens s'objecter en vertu du seul principe de protéger la vie privée. Je ne sais pas si vous avez écouté ces témoignages. Avez-vous l'impression qu'on met le droit à la vie privée de ces criminels devant le droit des enfants d'être protégés?

[*Traduction*]

Mme Schinas-Vlasis : Oui. Une réponse très courte : oui.

Le sénateur Baker : Je n'ai qu'une question pour les Clubs Garçons et Filles. Lorsque vous vous êtes présentés devant le comité de la Chambre des communes, vous avez recommandé que le projet de loi soit scindé. D'après l'exposé que vous présentez maintenant au comité du Sénat, vous ne semblez plus proposer cela, mais dire très fort : « Oui, protégez les enfants et les jeunes contre la cyberintimidation, mais vous devez également protéger leur droit à la vie privée. » Et vous suggérez non pas que nous scindions le projet de loi, mais que nous prêtions une attention particulière au commissaire à la protection de la vie privée et à ses recommandations. Ai-je raison de dire cela? Pourriez-vous en dire plus à ce sujet?

Ms. Gouin: We still think it would be a good idea to split the bill, but we recognize that that's not likely to happen. We're recommending we pay attention to the issues that were raised and the reason behind many requests to split the bill, one being that this bill is very large.

So while we are speaking to certain aspects of it based on our experience, there's a lot of the bill we can't speak to. We're counting on others to make sense of it and make sure it's a good, strong bill that will protect children and youth. If it were simpler and limited to just cyberbullying, that's all we've spoken about. For the rest, we're letting other people step up and speak to that. In that sense, it would be easier for us to fully support those provisions if it were split. Right now, we're doing our best with what we have.

Senator Baker: Congratulations on your presentations to the house committee and Senate committee.

Senator McInnis: I have a follow-up on this. On splitting the bill, you can't put something in the Criminal Code that does not have the procedure and process in order to bring about a charge for the police, so I fail to understand. I think you have to look at this bill in its entirety, because they need the thresholds put in place in order to investigate the crime. I don't get that point at all when you read this bill in its entirety. Why would we not want to have the investigative powers when we're putting the offence in place?

Ms. Gouin: Given that, we'll trust the judgment that this bill is moving forward together, as one, with the investigative powers, and you'll consider the issues that were raised with concerns to privacy. We won't be doing that, but that's why we took that part out of this brief.

Senator McInnis: Responsible governments have to weigh the balance.

Senator Batters: Mr. Alhattab, you suggested that we consult youth on this. I did my own personal small consultation last week when I was home in Regina. I was relaying this to witnesses yesterday. I spoke to a high school class of 22 students at Campbell Collegiate in Regina. I talked to them about different things, my role in the Senate and what I do. I was telling them about this committee and, given that it was Grade 10 students, cyberbullying could be something that they in particular are dealing with right now. Maybe somebody sitting in that class might be someone who is going through this right now. I talked to them a little bit about this bill and gave them some information about the needhelpnow.ca website, which we previously heard about from a police officer who was testifying before our committee.

Mme Gouin : Nous pensons encore que ce serait une bonne idée de scinder le projet de loi, mais nous croyons savoir qu'il est peu susceptible de l'être. Nous recommandons que vous prêtiez attention aux questions qui ont été soulevées et à la raison des nombreuses demandes faites pour que le projet de loi soit scindé, notamment le fait qu'il est très volumineux.

Donc, même si nous parlons de certains de ces aspects en fonction de notre expérience, il y a beaucoup d'aspects dont nous ne pouvons pas parler. Nous comptons sur d'autres intervenants pour en comprendre la logique et s'assurer qu'il s'agit d'un bon projet de loi solide qui protégera les enfants et les jeunes. S'il était plus simple et limité à la cyberintimidation... C'est tout ce dont nous avons parlé. Pour le reste, nous laissons les autres gens se manifester pour en parler. En ce sens, il serait plus facile pour nous d'appuyer pleinement ces dispositions s'il était scindé. Pour le moment, nous faisons de notre mieux avec ce que nous avons.

Le sénateur Baker : Félicitations pour les exposés que vous avez présentés aux comités de la Chambre et du Sénat.

Le sénateur McInnis : Je veux revenir là-dessus. Concernant la possibilité de scinder le projet de loi, on ne peut pas ajouter au Code criminel un élément qui n'a pas la procédure et le processus nécessaires pour permettre à la police de porter des accusations, alors je ne comprends pas. Je pense que vous devez regarder ce projet de loi en entier parce que les services de police ont besoin que les seuils soient mis en place pour enquêter sur le crime. Je ne comprends pas du tout cet argument, quand je l'envisage à la lumière du projet de loi en entier. Pourquoi ne voudrions-nous pas avoir les pouvoirs d'enquête si nous mettons en place l'infraction?

Mme Gouin : Alors, nous allons faire confiance au jugement selon lequel le projet de loi doit être adopté dans son ensemble, en un seul tenant, avec les pouvoirs d'enquête, et vous allez tenir compte des préoccupations qui ont été soulevées à l'égard de la protection de la vie privée. Nous n'allons pas le faire, mais c'est pourquoi nous avons isolé cette partie du texte.

Le sénateur McInnis : Les gouvernements responsables doivent peser le pour et le contre.

La sénatrice Batters : Monsieur Alhattab, vous avez proposé que nous consultions les jeunes à ce sujet. J'ai mené ma propre petite consultation personnelle la semaine dernière quand j'étais chez moi, à Regina. Je racontais cela aux témoins, hier. Je me suis adressée à une classe de 22 élèves du secondaire, au Campbell Collegiate, à Regina. Je leur ai parlé de diverses choses, de mon rôle au Sénat et de ce que je fais. Je leur ai parlé du comité et, comme il s'agissait d'élèves de 10e année, il est bien possible que l'intimidation soit un phénomène auquel ils font face personnellement, à l'heure actuelle. Peut-être qu'une personne assise dans cette classe en était victime à ce moment-là. Je leur ai parlé un peu de ce projet de loi, et je leur ai donné certaines informations au sujet du site web AidezMoiSVP.ca, dont nous avons déjà entendu parler par un agent de police qui a témoigné devant notre comité.

When I took questions after my presentation, there was one particular student who hadn't asked anything of me prior to that point. He was sitting in the front row and had listened attentively but hadn't asked anything. The teacher told the class: "This is your chance to influence a lawmaker. What do you think about this bill?" I asked them: "Do you think we need legislation? Do you think it's satisfactory to just have more public education and websites, that sort of thing?" This student said to me that he thought it was very important we have this law because without having a significant law like this, we wouldn't have consequences for these types of very serious actions.

I relay that to thank you for your comment. In our little part, we're trying to do that as well. Certainly we're receiving information as well, sometimes from email and phone calls.

Senator McIntyre: I want to go back to the idea of splitting the bill. I know this idea was discussed at length by the House of Commons committee, and they decided not to split the bill. However, they did recommend a parliamentary review in seven years. I wanted to have your thoughts on the seven-year review of this legislation.

Ms. Anderson: We've never been part of wanting to separate the bill, but I think a seven-year review would be good because technology will have changed in seven years. You might be looking at something completely different. A review in seven years would be a very good idea.

Senator McIntyre: You're in agreement with that recommendation?

Ms. Anderson: Yes.

The Chair: Thank you all for a very helpful and informative contribution to our deliberations on this important piece of legislation.

Members, we will continue discussing Bill C-13 next week. We also have on our agenda the pre-study element of the budget implementation act that we have to deal with in a timely way. We'll be looking at that next week as well.

The meeting is adjourned.

(The committee adjourned.)

Quand j'ai répondu à des questions après mon exposé, il y avait un élève en particulier, qui ne m'avait rien demandé jusqu'à ce moment-là. Il était assis dans la première rangée et avait écouté attentivement, mais il n'avait posé aucune question. L'enseignant a dit à la classe « C'est votre chance d'influencer un législateur. Que pensez-vous de ce projet de loi? » Je leur ai demandé : « Pensez-vous que nous avons besoin d'une loi? Selon vous, est-il satisfaisant de se contenter d'une plus grande sensibilisation publique et d'un plus grand nombre de sites web, de ce genre de choses? » Cet élève m'a dit qu'il pensait qu'il était très important que nous adoptions ce projet de loi parce que, sans une loi importante comme celle-ci, il n'y aurait pas de conséquences pour ces types d'actes très graves.

Je vous raconte cela pour vous remercier de votre commentaire. Dans notre petite région, nous essayons aussi de le faire. Il est certain que nous recevons également de l'information, parfois par courriel et sous forme d'appels téléphoniques.

Le sénateur McIntyre : Je veux revenir à l'idée de scinder le projet de loi. Je sais qu'elle a fait l'objet de discussions approfondies par le comité de la Chambre des communes et que les membres ont décidé de ne pas le scinder. Cependant, ils ont recommandé un examen parlementaire dans sept ans. J'aimerais entendre vos réflexions au sujet de l'examen du projet de loi dans sept ans.

Mme Anderson : Nous n'avons jamais fait partie des personnes qui veulent scinder le projet de loi, mais, selon moi, un examen dans sept ans serait une bonne chose, parce que, dans sept ans, la technologie aura changé. On pourrait observer une situation complètement différente. Un examen dans sept ans serait une très bonne idée.

Le sénateur McIntyre : Vous êtes d'accord avec cette recommandation?

Mme Anderson : Oui.

Le président : Je vous remercie tous de votre contribution très utile et instructive à nos délibérations sur cet important texte de loi.

Mesdames et messieurs, nous allons poursuivre la discussion sur le projet de loi C-13 la semaine prochaine. Nous avons également à notre ordre du jour l'étude préliminaire de la Loi d'exécution du budget, dont nous devons nous occuper rapidement. Nous allons étudier cette question la semaine prochaine également.

La séance est levée.

(La séance est levée.)

WITNESSES

Wednesday, November 19, 2014

Criminal Lawyers' Association:

Leo Russomanno, Member and Criminal Defence Counsel;

Michael Spratt, Member and Criminal Defence Counsel.

Canadian Centre for Child Protection:

Lianna McDonald, Executive Director;

Monique St. Germain, General Counsel.

As individuals:

Andrea Slane, Associate Professor, University of Ontario Institute of Technology;

Michael Geist, Law Professor, University of Ottawa.

Thursday, November 20, 2014

Canadian Bar Association:

Tony Paisana, Executive Member, Criminal Justice Section (by video conference).

Office of the Privacy Commissioner of Canada:

Daniel Therrien, Privacy Commissioner of Canada;

Patricia Kosseim, Senior General Counsel and Director General;

Daniel Caron, Legal Counsel.

Boys and Girls Clubs of Canada:

Rachel Gouin, Director, Research and Public Policy;

Fahd Alhattab, Alumnus.

Bully Free Community Alliance:

Basiliki Schinas-Vlasis, Co-Founder;

Gwyneth Anderson, Co-Founder.

TÉMOINS

Le mercredi 19 novembre 2014

Criminal Lawyers' Association :

Leo Russomanno, membre et criminaliste;

Michael Spratt, membre et criminaliste.

Centre canadien de protection de l'enfance :

Lianna McDonald, directrice exécutive;

Monique St. Germain, avocate-conseil.

À titre personnel :

Andrea Slane, professeure agrégée, Institut universitaire de technologie de l'Ontario;

Michael Geist, professeur de droit, Université d'Ottawa.

Le jeudi 20 novembre 2014

Association du Barreau canadien :

Tony Paisana, membre de l'exécutif, Section du droit pénal (par vidéoconférence).

Commissariat à la protection de la vie privée du Canada :

Daniel Therrien, commissaire à la protection de la vie privée du Canada;

Patricia Kosseim, avocate générale principale et directrice générale;

Daniel Caron, conseiller juridique.

Clubs Garçons et Filles du Canada :

Rachel Gouin, directrice, recherche et politiques publiques;

Fahd Alhattab, ancien membre.

Bully Free Community Alliance :

Basiliki Schinas-Vlasis, cofondatrice;

Gwyneth Anderson, cofondatrice.