



Third Session
Fortieth Parliament, 2010-11

SENATE OF CANADA

*Proceedings of the Standing
Senate Committee on*

**Legal and
Constitutional Affairs**

Chair:
The Honourable JOAN FRASER

Wednesday, February 16, 2011
Thursday, February 17, 2011

Issue No. 21

Third and fourth (final) meetings on:
Bill C-22, An Act respecting the mandatory
reporting of Internet child pornography by persons
who provide an Internet service

INCLUDING:
THE FIFTEENTH REPORT OF THE COMMITTEE
(Bill C-22, An Act respecting the mandatory
reporting of Internet child pornography by persons
who provide an Internet service)

WITNESSES:
(*See back cover*)

Troisième session de la
quarantième législature, 2010-2011

SÉNAT DU CANADA

*Délibérations du Comité
sénatorial permanent des*

**Affaires juridiques et
constitutionnelles**

Présidente :
L'honorable JOAN FRASER

Le mercredi 16 février 2011
Le jeudi 17 février 2011

Fascicule n° 21

Troisième et quatrième (dernière) réunions concernant :
Le projet de Loi C-22, Loi concernant la déclaration
obligatoire de la pornographie juvénile sur Internet par
les personnes qui fournissent des services Internet

Y COMPRIS :
LE QUINZIÈME RAPPORT DU COMITÉ
(Projet de Loi C-22, Loi concernant la déclaration
obligatoire de la pornographie juvénile sur Internet par
les personnes qui fournissent des services Internet)

TÉMOINS :
(*Voir à l'endos*)

STANDING SENATE COMMITTEE ON
LEGAL AND CONSTITUTIONAL AFFAIRS

The Honourable Joan Fraser, *Chair*

The Honourable John D. Wallace, *Deputy Chair*

and

The Honourable Senators:

Angus	Joyal, P.C.
Boisvenu	* LeBreton, P.C.
Carignan	(or Comeau)
Chaput	Meredith
* Cowan	Munson
(or Tardif)	Raine
Dallaire	Runciman

* Ex officio members

(Quorum 4)

Changes in membership of the committee:

Pursuant to rule 85(4), membership of the committee was amended as follows:

The Honourable Senator Dallaire replaced the Honourable Senator Watt (*February 17, 2011*).

The Honourable Senator Meredith replaced the Honourable Senator Rivest (*February 17, 2011*).

The Honourable Senator Raine replaced the Honourable Senator Lang (*February 17, 2011*).

The Honourable Senator Lang replaced the Honourable Senator Neufeld (*February 16, 2011*).

The Honourable Senator Neufeld replaced the Honourable Senator Lang (*February 16, 2011*).

The Honourable Senator Munson replaced the Honourable Senator Baker, P.C. (*February 16, 2011*).

The Honourable Senator Angus replaced the Honourable Senator Stratton (*February 10, 2011*).

COMITÉ SÉNATORIAL PERMANENT DES
AFFAIRES JURIDIQUES ET CONSTITUTIONNELLES

Présidente : L'honorable Joan Fraser

Vice-président : L'honorable John D. Wallace

et

Les honorables sénateurs :

Angus	Joyal, C.P.
Boisvenu	* LeBreton, C.P.
Carignan	(ou Comeau)
Chaput	Meredith
* Cowan	Munson
(ou Tardif)	Raine
Dallaire	Runciman

* Membres d'office

(Quorum 4)

Modifications de la composition du comité :

Conformément à l'article 85(4) du Règlement, la liste des membres du comité est modifiée, ainsi qu'il suit :

L'honorable sénateur Dallaire a remplacé l'honorable sénateur Watt (*le 17 février 2011*).

L'honorable sénateur Meredith a remplacé l'honorable sénateur Rivest (*le 17 février 2011*).

L'honorable sénateur Raine a remplacé l'honorable sénateur Lang (*le 17 février 2011*).

L'honorable sénateur Lang a remplacé l'honorable sénateur Neufeld (*le 16 février 2011*).

L'honorable sénateur Neufeld a remplacé l'honorable sénateur Lang (*le 16 février 2011*).

L'honorable sénateur Munson a remplacé l'honorable sénateur Baker, C.P. (*le 16 février 2011*).

L'honorable sénateur Angus a remplacé l'honorable sénateur Stratton (*le 10 février 2011*).

MINUTES OF PROCEEDINGS

OTTAWA, Wednesday, February 16, 2011
(48)

[*English*]

The Standing Senate Committee on Legal and Constitutional Affairs met this day, at 4:19 p.m., in room 257, East Block, the chair, the Honourable Joan Fraser, presiding.

Members of the committee present: The Honourable Senators Angus, Boisvenu, Carignan, Chaput, Fraser, Joyal, P.C., Munson, Neufeld, Runciman, Wallace and Watt (11).

In attendance: Laura Barnett and Marcia Jones, Analysts, 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 Tuesday, February 8, 2011, the committee continued its consideration of Bill C-22, An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service. (*For complete text of the order of reference, see proceedings of the committee, Issue No. 21.*)

WITNESSES:

Office of the Privacy Commissioner of Canada:

Chantal Bernier, Assistant Privacy Commissioner;

Anna Zubrzycka, Policy Analyst, Legal Services, Policy and Parliamentary Affairs Branch.

Canadian Centre for Child Protection:

Lianna McDonald, Executive Director;

Signy Arnason, Director, Cybertip.ca;

Ontario Provincial Police:

Inspector Scott Naylor, Child Sexual Exploitation Section.

Canadian Association of Chiefs of Police:

Vincent Westwick, General Counsel.

ExitCertified:

Michael MacKay, Senior Consultant.

UNICEF Canada:

Marvin Bernstein, Chief Advisor, Advocacy.

Kids Internet Safety Alliance:

Paul Gillespie, President and Chief Executive Officer.

The chair made an opening statement.

PROCÈS-VERBAUX

OTTAWA, le mercredi 16 février 2011
(48)

[*Traduction*]

Le Comité sénatorial permanent des affaires juridiques et constitutionnelles se réunit aujourd'hui, à 16 h 19, dans la pièce 257 de l'édifice de l'Est, sous la présidence de l'honorable Joan Fraser (*présidente*).

Membres du comité présents : Les honorables sénateurs Angus, Boisvenu, Carignan, Chaput, Fraser, Joyal, C.P., Munson, Neufeld, Runciman, Wallace et Watt (11).

Également présentes : Laura Barnett et Marcia Jones, analystes, 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 mardi 8 février 2011, le comité poursuit son examen du projet de loi C-22, Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet. (*Le texte intégral de l'ordre de renvoi figure au fascicule n° 21 des délibérations comité.*)

TÉMOINS :

Commissariat à la protection de la vie privée du Canada :

Chantal Bernier, commissaire adjointe à la protection de la vie privée;

Anna Zubrzycka, analyste politique, Direction des services juridiques, des politiques et des affaires parlementaires.

Centre canadien de protection de l'enfance :

Lianna McDonald, directrice générale;

Signy Arnason, directrice, Cyberaide.ca.

Police provinciale de l'Ontario :

Inspecteur Scott Naylor, Unité de la pornographie juvénile.

Association canadienne des chefs de police :

Vincent Westwick, avocat général.

ExitCertified :

Michael MacKay, consultant principal.

UNICEF Canada :

Marvin Bernstein, conseiller principal, Promotion et défense des droits.

Kids Internet Safety Alliance :

Paul Gillespie, président-directeur général.

Le président ouvre la séance.

The Honourable Senator Chaput moved:

That the following material be filed as exhibits with the Clerk of the Committee:

- Response from Catherine Latimer and Paul Saint-Denis, Justice Canada, to a question taken on notice at the October 21, 2010 meeting, relating to Bill S-10. (Exhibit 1120-04-02-3.40/L1-S-10, 13, “3”)
- Response from the Honourable Vic Toews, P.C., M.P., Minister of Public Safety to a question taken on notice by witnesses Shelley Trevethan, Denis Ladouceur and Anne Gagné, Public Safety Canada, at the October 6, 2010 meeting, relating to the Parole Board of Canada’s proposal under the *User Fees Act*. (Exhibit 1120-04-02-3.40/L1-SS-2,12,“1”)
- Letter from the Honourable Ross Landry, Attorney General of Nova Scotia, relating to Bill C-22. (Exhibit 1120-04-02-3.40/L1-C-22, 21, “1”)
- Letter from Mr. Thomas Copeland, Chair, Canadian Association of Internet Providers, relating to Bill C-22. (Exhibit 1120-04-02-3.40/L1-C-22, 21, “2”)
- Letter from Ms. Pamela Dinsmore, Vice President, Regulatory, Rogers Communications Inc., relating to Bill C-22. (Exhibit 1120-04-02-3.40/L1-C-22, 21, “3”)
- Letter from Barreau du Québec, relating to Bill C-22. (Exhibit 1120-04-02-3.40/L1-C-22, 21, “4”)
- Brief from the Honourable Andrew Swan, Minister of Justice and Attorney General of Manitoba, relating to Bill C-22. (Exhibit 1120-04-02-3.40/L1-C-22, 21, “5”)
- Letter from Mr. Craig McTaggart, Director, Broadband Polycys, TELUS, relating to Bill C-22. (Exhibit 1120-04-02-3.40/L1-C-22, 21, “6”)
- Response from Catherine Kane, Justice Canada, to a question taken on notice at the February 9, 2011 meeting, relating to Bill C-22. (Exhibit 1120-04-02-3.40/L1-C-22, 21, “7”)
- Response from Catherine Kane, Justice Canada, to a question taken on notice at the February 9, 2011 meeting, relating to Bill C-22. (Exhibit 1120-04-02-3.40/L1-C-22, 21, “8”)

The question being put on the motion, it was adopted.

Ms. Bernier made an opening statement and answered questions.

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

At 5:23 p.m., the committee resumed.

Ms. McDonald, Inspector Naylor and Mr. Westwick each made a statement and, together with Ms. Arnason, answered questions.

L’honorable sénateur Chaput propose :

Que les documents suivants soient déposés auprès de la greffière du comité :

- Réponse de Catherine Latimer et de Paul Saint-Denis, Justice Canada, à une question prise en note lors de la réunion du 21 octobre 2010 concernant le projet de loi S-10. (pièce 1120-04-02-3.40/L1-S-10, 13, « 3 »)
- Réponse de l’honorable Vic Toews, C.P., député, ministre de la Sécurité publique, à une question prise en note par Shelley Trevethan, Denis Ladouceur et Anne Gagné, Sécurité publique Canada, lors de la réunion du 6 octobre 2010, concernant la proposition mise de l’avant par la Commission des libérations conditionnelles et visant la Loi sur les frais d’utilisation. (pièce 1120-04-02-3.40/L1-SS-2,12, « 1 »)
- Lettre de l’honorable Ross Landry, procureur général de la Nouvelle-Écosse, concernant le projet de loi C-22. (pièce 1120-04-02-3.40/L1-C-22, 21, « 1 »)
- Lettre de M. Thomas Copeland, président, Association canadienne des fournisseurs Internet, concernant le projet de loi C-22. (pièce 1120-04-02-3.40/L1-C-22, 21, « 2 »)
- Lettre de Mme Pamela Dinsmore, vice-présidente, Affaires réglementaires, Rogers Communications Inc., concernant le projet de loi C-22. (pièce 1120-04-02-3.40/L1-C-22, 21, « 3 »)
- Lettre du Barreau du Québec concernant le projet de loi C-22 (pièce 1120-04-02-3.40/L1-C-22, 21, « 4 »)
- Mémoire présenté par l’honorable Andrew Swan, ministre de la Justice et procureur général du Manitoba, concernant le projet C-22. (pièce 1120-04-02-3.40/L1-C-22, 21, « 5 »)
- Lettre de M. Craig McTaggart, directeur, Politique de large bande, TELUS, concernant le projet de loi C-22. (pièce 1120-04-02-3.40/L1-C-22, 21, « 6 »)
- Réponse de Catherine Kane, Justice Canada, à une question prise en note lors de la réunion du 9 février 2011 concernant la projet de loi C-22. (pièce 1120-04-02-3.40/L1-C-22, 21, « 7 »)
- Réponse de Catherine Kane, Justice Canada, à une question prise en note lors de la réunion du 9 février 2011 concernant le projet de C-22. (pièce 1120-04-02-3.40/L1-C-22, 21, « 8 »)

La motion, mise aux voix, est adoptée.

Mme Bernier fait une déclaration, puis répond aux questions.

À 17 h 15, la séance est suspendue.

À 17 h 23, la séance reprend.

Mme McDonald, M. Naylor et M. Westwick font une déclaration, puis de concert avec Mme Arnason, répondent aux questions.

At 6:18 p.m., the committee suspended.

At 6:25 p.m., the committee resumed.

Mr. MacKay made a statement and answered questions.

At 7:13 p.m., the committee suspended.

At 7:15 p.m., the committee resumed.

Mr. Bernstein and Mr. Gillespie each made a statement and answered questions.

At 7:58 p.m., the committee adjourned to the call of the chair.

ATTEST:

OTTAWA, Thursday, February 17, 2011
(49)

[*English*]

The Standing Senate Committee on Legal and Constitutional Affairs met this day, at 10:37 a.m., in room 257, East Block, the chair, the Honourable Joan Fraser, presiding.

Members of the committee present: The Honourable Senators Angus, Boisvenu, Carignan, Chaput, Dallaire, Fraser, Joyal, P.C., Meredith, Munson, Raine, Runciman, and Wallace (12).

In attendance: Laura Barnett and Marcia Jones, Analysts, 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 Tuesday, February 8, 2011, the committee continued its consideration of Bill C-22, An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service. (*For complete text of the order of reference, see proceedings of the committee, Issue No. 21.*)

It was agreed that the committee proceed to clause-by-clause consideration of Bill C-22, An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service.

It was agreed that the title stand postponed.

It was agreed that clause 1 carry.

It was agreed that clause 2 carry.

It was agreed that clause 3 carry.

It was agreed that clause 4 carry, on division.

It was agreed that clause 5 carry.

It was agreed that clause 6 carry, on division.

It was agreed that clause 7 carry.

It was agreed that clause 8 carry.

À 18 h 18, la séance est suspendue.

À 18 h 25, la séance reprend.

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

À 19 h 13, la séance est suspendue.

À 19 h 15, la séance reprend.

M. Bernstein et Gillespie font une déclaration, puis répondent aux questions.

À 19 h 58, le comité suspend ses travaux jusqu'à nouvelle convocation de la présidence.

ATTESTÉ :

OTTAWA, le jeudi 17 février 2011
(49)

[*Traduction*]

Le Comité sénatorial permanent des affaires juridiques et constitutionnelles se réunit aujourd'hui, à 10 h 37, dans la pièce 257 de l'Édifice de l'Est, sous la présidence de l'honorable Joan Fraser (*présidente*).

Membres du comité présents : Les honorables sénateurs Angus, Boisvenu, Carignan, Chaput, Dallaire, Fraser, Joyal, C.P., Meredith, Munson, Raine, Runciman, et Wallace (12).

Également présentes : Laura Barnett et Marcia Jones, analystes, 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 mardi 8 février 2011, le comité poursuit son examen du projet de loi C-22, Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet. (*Le texte intégral de l'ordre de renvoi figure au fascicule n° 21 des délibérations du comité.*)

Il est convenu que le comité procède à l'étude article par article du projet de loi C-22, Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet.

Il est convenu de reporter l'étude du titre.

Il est convenu d'adopter l'article 1.

Il est convenu d'adopter l'article 2.

Il est convenu d'adopter l'article 3.

Il est convenu d'adopter l'article 4, avec dissidence.

Il est convenu d'adopter l'article 5.

Il est convenu d'adopter l'article 6, avec dissidence.

Il est convenu d'adopter l'article 7.

Il est convenu d'adopter l'article 8.

It was agreed that clause 9 carry.

It was agreed that clause 10 carry.

It was agreed that clause 11 carry.

It was agreed that clause 12 carry.

It was agreed that clause 13 carry.

It was agreed that the title carry.

It was agreed that the bill carry, on division.

At 10:46 a.m., it was agreed that, pursuant to rule 92(2)(f), the committee proceed in camera to discuss draft observations.

It was agreed that Senators' staff be allowed to remain in the room for the in camera portion of today's meeting.

It was agreed that observations be appended to the committee's report on the bill.

It was agreed that the Subcommittee on Agenda and Procedure be empowered to approve the final version of the observations, taking into consideration today's discussion, and with any necessary editorial, grammatical and translation changes required.

It was agreed that the chair report the bill with observations to the Senate.

It was agreed that the following material be filed as exhibits with the Clerk of the Committee:

- Letter from Mr. Timothy Sparapani, Director, Public Policy, Facebook, relating to Bill C-22. (Exhibit 1120-04-02-3.40/L1-C-22, 21, "9")

At 11:25 a.m., the committee adjourned to the call of the chair.

ATTEST:

La greffière du comité,

Shaila Anwar

Clerk of the Committee

Il est convenu d'adopter l'article 9.

Il est convenu d'adopter l'article 10.

Il est convenu d'adopter l'article 11.

Il est convenu d'adopter l'article 12.

Il est convenu d'adopter l'article 13.

Il est convenu d'adopter le titre.

Il est convenu d'adopter le projet de loi, avec dissidence.

À 10 h 46, conformément à l'article 92(2)f) du Règlement, le comité se réunit à huis clos pour examiner l'ébauche d'observations.

Il est convenu d'autoriser le personnel des sénateurs à rester dans la salle pendant le huis clos.

Il est convenu d'annexer les observations au rapport du comité.

Il est convenu que le Sous-comité du programme et de la procédure soit autorisé à approuver la version finale des observations, compte tenu des discussions qui ont eu lieu aujourd'hui, et à y apporter les changements de forme, grammaticaux ou de traduction nécessaires.

Il est convenu que le président fasse rapport du projet de loi, avec les observations, au Sénat.

Il est convenu que les documents suivants soient déposés auprès de la greffière du comité :

- Lettre de M. Timothy Sparapani, directeur, Politique publique, Facebook, concernant le projet de loi C-22. (pièce 1120-04-02-3.40/L1-C-22, 21, « 9 »)

À 11 h 25, le comité suspend ses travaux jusqu'à nouvelle convocation de la présidence.

ATTESTÉ :

REPORT OF THE COMMITTEE

Tuesday, March 1, 2011

The Standing Senate Committee on Legal and Constitutional Affairs has the honour to present its

FIFTEENTH REPORT

Your committee, to which was referred Bill C-22, An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service, has, in obedience to the order of reference of Tuesday, February 8, 2011, examined the said Bill and now reports the same without amendment

Your committee has also made certain observations, which are appended to this report.

Respectfully submitted,

La présidente,

JOAN FRASER

Chair

OBSERVATIONS**to the Fifteenth Report of the Standing Senate Committee on Legal and Constitutional Affairs**

After receiving testimony from a broad spectrum of witnesses, including police services, government officials, Internet service providers, technical advisors, children's rights advocates, academics, and those who currently monitor child pornography on the Internet, the committee is deeply concerned about the incredible proliferation of Internet child pornography. Tens of thousands of new images or videos are posted on the Internet every week and it is estimated that there are currently more than 5 million unique child sexual abuse images on the Internet. An estimated 500,000 individuals worldwide are actively involved in the trafficking of child sexual abuse images on the Internet. This is a crime of truly devastating proportions.

In this regard, witnesses appearing before the committee advised that in their opinions, technology now exists which would significantly assist in addressing, and in some cases eliminating, this scourge.

Bill C-22 is one means to assist the criminal justice system in keeping pace with technological advances while respecting Canadians' rights. As a next step, the committee now urges the Minister to act expeditiously to inquire into the technologies available to combat child pornography on the Internet, to explore the further development and utilization of such technologies and, in so doing, to work with all relevant partners, including international partners, to make such technologies more widely available. The committee would appreciate being kept informed of developments in this regard.

RAPPORT DU COMITÉ

Le mardi 1^{er} mars 2011

Le Comité sénatorial permanent des affaires juridiques et constitutionnelles a l'honneur de présenter son

QUINZIÈME RAPPORT

Votre comité auquel a été renvoyé le projet de loi C-22, Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet, a, conformément à l'ordre de renvoi du mardi 8 février 2011, examiné ledit projet de loi et en fait maintenant rapport sans amendement.

Votre comité a aussi fait certaines observations qui sont annexées au présent rapport.

Respectueusement soumis,

OBSERVATIONS**annexées au quinzième rapport du Comité sénatorial permanent des affaires juridiques et constitutionnelles**

Après avoir entendu un large éventail de témoins, y compris des représentants des services de police, du gouvernement, ainsi que des fournisseurs de services Internet, des conseillers techniques, des défenseurs des droits des enfants, des académiciens et des responsables de la surveillance de la pornographie juvénile sur Internet, le comité est très préoccupé par l'ampleur du problème de la pornographie juvénile sur Internet. Des dizaines de milliers de nouvelles images ou de nouveaux vidéos sont téléchargés sur Internet chaque semaine, et on estime qu'il y a actuellement plus de 5 millions d'images d'exploitation sexuelle d'enfants sur Internet. Quelque 500 000 individus dans le monde participent activement au trafic de telles images. Il s'agit d'un crime qui prend des proportions extrêmement inquiétantes.

À cet égard, les témoins qui ont comparu devant le comité ont dit qu'il existe maintenant des technologies qui pourraient être très utiles pour régler, voire éliminer dans certains cas, ce fléau.

Le projet de loi C-22 est un moyen d'aider le système de la justice criminelle à suivre l'évolution technologique tout en respectant les droits des Canadiens. La prochaine étape pour le comité consistera à exhorter le ministre à se renseigner immédiatement sur les technologies disponibles pour lutter contre la pornographie juvénile sur Internet, à se pencher sur le développement et l'utilisation de ces technologies et, à cette fin, à travailler de concert avec tous les partenaires appropriés, dont des partenaires internationaux, pour rendre ces technologies plus accessibles. Le comité aimerait être tenu au courant de tout fait nouveau dans ce dossier.

EVIDENCE

OTTAWA, Wednesday, February 16, 2011

The Standing Senate Committee on Legal and Constitutional Affairs, to which was referred Bill C-22, An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service, met this day at 4:19 p.m. to give consideration to the bill.

Senator Joan Fraser (*Chair*) in the chair.

[*English*]

The Chair: Before we turn to the main agenda item of the day, which is continuing the study of Bill C-22, I will ask for a motion. You have all received 10 documents that have been submitted to the committee, including a number of responses from the justice ministry. You all have a list of those documents. Might I have a motion that these documents be filed as exhibits with the clerk?

Senator Chaput: I so move.

The Chair: So moved, by Senator Chaput. All in favour? Opposed? Abstentions? Carried.

[*Translation*]

It is a very great pleasure today to welcome from, the Office of the Privacy Commissioner of Canada, Ms. Chantal Bernier, who is Assistant Privacy Commissioner, and Ms. Anna Zubrzycka, Policy Analyst, Legal Services, at the Office of the Privacy Commissioner of Canada.

[*English*]

Thank you both for being here.

[*Translation*]

Honourable senators, since we have a lot of witnesses to hear today, I would ask you to be concise with your questions.

I believe Ms. Bernier has an opening statement to make. You may begin, madam.

Chantal Bernier, Assistant Privacy Commissioner, Office of the Privacy Commissioner of Canada: Thank you, Madam Chair, for inviting me to present the perspective of the Office of the Privacy Commissioner of Canada on Bill C-22.

I applaud the government for moving to curb the prevalence of online child pornography, a profoundly repellent scourge that makes victims of our society's most vulnerable. Every child has inherent human rights and warrants special care and protection.

TÉMOIGNAGES

OTTAWA, le mercredi 16 février 2011

Le Comité sénatorial permanent des affaires juridiques et constitutionnelles, à qui a été renvoyé le projet de loi C-22, Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet, se réunit aujourd'hui à 16 h 19 pour procéder à l'étude du projet de loi.

Le sénateur Joan Fraser (*présidente*) occupe le fauteuil.

[*Traduction*]

La présidente : Avant de passer au principal point de l'ordre du jour, qui est la poursuite de l'étude du projet de loi C-22, je vous demande d'adopter une motion. Vous avez tous reçu 10 documents qui ont été remis au comité, notamment un certain nombre de réponses provenant du ministère de la Justice. Vous avez tous une liste de ces documents. Quelqu'un veut-il présenter une motion portant que ces documents soient déposés à titre de pièces auprès de la greffière.

Le sénateur Chaput : Je le propose.

La présidente : Le sénateur Chaput le propose. Tous ceux qui sont en faveur? Contre? Abstentions? Adopté.

[*Français*]

Nous avons le très grand plaisir aujourd'hui d'accueillir du Commissariat à la protection de la vie privée du Canada, Mme Chantal Bernier, qui est commissaire adjointe à la protection de la vie privée, ainsi que Mme Anna Zubrzycka, qui est analyste politique aux Services juridiques au Commissariat à la protection de la vie privée du Canada.

[*Traduction*]

Je vous remercie toutes les deux d'être venues.

[*Français*]

Honorables sénateurs, puisque nous avons beaucoup de témoins à entendre aujourd'hui je vous prierais d'être concis dans vos questions.

Je crois que Mme Bernier a une déclaration liminaire à faire. Alors vous pouvez commencer, madame.

Chantal Bernier, commissaire adjointe à la protection de la vie privée, Commissariat à la protection de la vie privée du Canada : Merci, madame la présidente, de m'avoir invitée à présenter le point de vue du Commissariat à la protection de la vie privée du Canada sur le projet de loi C-22.

Je félicite le gouvernement d'avoir pris des mesures pour mettre fin à l'offre croissante de pornographie juvénile en ligne, ce fléau dont les victimes sont véritablement les membres les plus vulnérables de notre société. Tous les enfants possèdent des droits inhérents tels que ceux d'être protégé et de recevoir des soins adéquats.

This was the message of the 1989 Convention on the Rights of the Child, a message the Canadian government reaffirmed by ratifying the Convention and its Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography.

The Office of the Privacy Commissioner of Canada has been taking action in that regard. In 2008, in the context of an international conference of data protection and privacy commissioners, Commissioner Stoddart sponsored a resolution on children's online privacy. This resolution called for legislation to limit the collection, use and disclosure of children's personal information.

In 2009, under the auspices of the International Development Research Centre, the Office of the Privacy Commissioner of Canada, contributed to the drafting of the Memorandum of Montevideo on the protection of children's and adolescents' personal data and privacy on the Internet.

In that context, I am pleased that Parliament is now considering legislation to combat child pornography. The intent is entirely laudable.

My intent here today is to submit a few questions for your deliberation, in the hope that Parliament will fashion an even better, more effective tool.

[English]

My first question relates to the implications of obliging a greater number of organizations to report — specifically, by widening this obligation to several organizations, are we actually further jeopardizing children who have already been victimized? Let me explain.

The bill obliges ISPs, Internet service providers, to report tips they receive from individuals about possible child pornography offences to a designated organization. From a review of *House of Commons Debates*, it appears that the designated organization would be Cybertip, a non-profit volunteer organization supported by the Government of Canada and such telecommunications giants as Bell, Rogers, Telus and Shaw.

Cybertip already receives tips from the public, assesses them and forwards to the police all those that are suspected to be unlawful. They have been at it since 2002 and, by all accounts, they are doing a great job. If the public can, and plainly does, already report to Cybertip, why would we wish to introduce another layer to the reporting process? By involving ISPs, do we simply expose these images to yet more eyes? By invading the privacy of these children, are we further victimizing them?

C'est ce que convoie la Convention relative aux droits de l'enfant en 1989, une convention que le Canada a ratifiée et qui comporte également un protocole facultatif concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants.

Le Commissariat à la protection de la vie privée du Canada a d'ailleurs fait ses propres efforts en ce sens. En 2008, dans le cadre d'une rencontre internationale des commissaires à la protection des données personnelles, la commissaire Stoddart a parrainé la Résolution sur la vie privée des enfants en ligne. Cette résolution réclame une législation qui poserait des limites à l'égard de la collecte, de l'utilisation et de la diffusion de renseignements personnels concernant les enfants.

En 2009, le Commissariat à la protection de la vie privée du Canada a participé à la rédaction du mémorandum de Montevideo qui était à ce moment développé sous l'égide du Centre de recherche pour le développement international, qui portait sur la protection du droit à la vie privée des enfants et des adolescents sur Internet.

Dans ces circonstances, vous comprendrez que je suis heureuse de constater que le Parlement envisage la mise sur pied d'une législation qui vise à combattre la pornographie juvénile. Le but en est tout à fait louable.

J'ai l'intention, aujourd'hui, de vous soumettre quelques questions, dans l'espoir que le Parlement élabore en fait un outil encore plus efficace.

[Traduction]

Ma première question concerne les répercussions que pourrait avoir le fait d'obliger un grand nombre d'organisations à signaler ce genre de cas — plus précisément, en étendant cette obligation à plusieurs organismes, ne risquons-nous pas de mettre encore en danger des enfants qui ont déjà été victimisés? Je m'explique.

Le projet de loi oblige les FSI, les fournisseurs de services Internet, à communiquer à un organisme désigné les renseignements qu'ils reçoivent au sujet d'infractions relatives à la pornographie juvénile. Il ressort de l'examen des *Débats de la Chambre des communes*, que l'organisation désignée serait Cyberaide, une organisation bénévole sans but lucratif soutenue par le gouvernement du Canada et des géants des télécommunications comme Bell, Rogers, Telus et Shaw.

Cyberaide reçoit déjà des renseignements du public, les évalue et transmet aux services de police tous ceux dont on soupçonne qu'ils concernent une activité illégale. Cet organisme fait ce travail depuis 2002 et, d'après tous les rapports, fait de l'excellent travail. Si le public peut déjà signaler ce genre de chose à Cyberaide, et il le fait déjà, pourquoi vouloir ajouter une autre étape au processus de déclaration? En faisant intervenir les FSI, ne risquons-nous pas simplement de montrer ces images à d'autres personnes? Cette atteinte à la vie privée de ces enfants ne risque-t-elle pas de les victimiser davantage?

My second question relates to the organizations that will be reporting these offences. Specifically, are they best suited for the task? This question centres on the effectiveness of the bill as currently drafted. Effective legislation would make the best and most appropriate institutions of our society responsible for stamping out child pornography, and these institutions must be equipped with the expertise and supports necessary to swiftly and efficiently enforce the law.

As you know, the bill would require an ISP to notify police if it has reasonable grounds to believe that an Internet service is, or has been, used to commit a child pornography offence. Who are these ISPs? Do they have the necessary expertise to enforce the law?

It is conceivable that major telecommunications companies do. They have teams of lawyers who are able to develop the legal knowledge, skills and resources necessary to provide useful assistance to police in this regard. However, we understand that the bill would also make cyber cafés, hotels, mom-and-pop restaurants and public libraries responsible for policing child pornography. Do they have the necessary expertise and do they have the resources to do so?

Consider, for example, that they would need to apply “reasonable grounds to believe” that an offence is being committed. This is a nuanced legal concept that could be difficult for the layperson to apply. Yet, even in the absence of specific legal training or support, all ISPs would be expected to assess what it means. Are mistakes likely? They are certainly possible, given the legislation would make reporting mandatory.

At the very least, I would caution, there will be an impulse to over report. We have observed this tendency in our audit of FINTRAC, Financial Transactions and Reports Analysis Centre of Canada. Where banks, casinos and other money-handling organizations are required to report suspicious transactions, employees are more likely to report even innocent interactions because the penalties for non-compliance are steep.

My third question relates to accountability. I want to underscore that my chief concern is that the legislation protect the interests of the child. In order to fully safeguard those interests, we also need a well-functioning society where the rule of law is paramount. For that reason, I am concerned when I see that Bill C-22 also obliges ISPs to seize and preserve all suspected computer data for 21 days without a police request or a warrant. Since the legislation does not define exactly what information the ISP must preserve, they can preserve anything from anyone, without the knowledge of the owners of the information and without judicial oversight.

Ma deuxième question se rapporte aux organismes qui déclareront ces infractions. Sont-ils les mieux désignés pour s’acquitter de cette tâche? Cette question concerne au premier chef l’efficacité du projet de loi dans sa version actuelle. Une législation efficace désignerait, comme responsables de l’éradication de la pornographie infantile, les autorités qui possèdent les compétences et les ressources nécessaires pour jouer ce rôle adéquatement. Elle prévoirait que ces institutions soient pourvues de l’expertise et de l’appui nécessaires pour appliquer la loi de façon rapide et efficace.

Comme vous le savez, le projet de loi oblige tout FSI à informer la police s’il a des motifs raisonnables de croire qu’un service Internet est, ou a été, utilisé, pour la perpétration d’une infraction relative à la pornographie juvénile. Qui sont ces FSI? Possèdent-ils l’expertise nécessaire pour appliquer la loi?

Il est tout à fait concevable que les principales compagnies de télécommunication, qui ont leur propre équipe d’avocats, puissent mettre en place les connaissances, les compétences et les ressources juridiques nécessaires pour assister efficacement la police à ce sujet. Le projet de loi conférerait toutefois aux cybercafés, aux hôtels, aux restaurants familiaux et aux bibliothèques publiques la responsabilité de contrôler la pornographie juvénile. Ces derniers possèdent-ils l’expertise ou les ressources nécessaires pour exercer ce rôle?

Prenons, par exemple, le fait qu’ils doivent invoquer « des motifs raisonnables de croire » qu’une infraction a été commise; cette expression renvoie à un concept juridique subtil qui peut être difficile à appliquer pour un non-initié. Et pourtant, même sans formation ni appui juridiques particuliers, les FSI devront manier et mettre en pratique cette notion. Cela entraînera-t-il un risque d’erreur? Sans aucun doute, puisque la déclaration serait obligatoire aux termes de la loi.

À tout le moins, je ferais une mise en garde contre les risques de surdéclaration. Nous avons été témoins de cette tendance dans le cadre de notre vérification du CANAFE, Centre d’analyse des opérations et déclarations financières du Canada. Dans les banques, les casinos et autres organisations manipulant de l’argent, qui sont tenus de déclarer les transactions douteuses, les employés font preuve d’une propension plus marquée, vu la sévérité des sanctions en cas de non-conformité, à déclarer des interactions non frauduleuses.

Ma troisième question a trait à la reddition de comptes. Je voudrais réitérer que ma première préoccupation est de veiller à ce que la loi protège les intérêts des enfants. Dans le but de préserver l’intégralité de ces intérêts, nous avons également besoin d’une société hautement fonctionnelle où règne la primauté du droit. D’où mes préoccupations à l’idée que le projet de loi C-22 oblige les FSI à saisir et à conserver toute donnée informatique suspecte pendant 21 jours, et ce, sans demande présentée par la police et sans mandat. Étant donné que la loi ne définit pas de manière exacte les renseignements que les FSI peuvent conserver, ceux-ci peuvent détenir n’importe quoi, venant de n’importe qui, et ce, à l’insu des propriétaires des renseignements et sans aucune surveillance juridique.

In contrast, if and when police are notified — by an ISP, by Cybertip or by any member of the public — about suspicious material, an orderly and verifiable record of events is established. Accountability, therefore, should remain where it belongs, namely, with the law enforcement agencies. This best serves the interests of children and society as a whole.

[Translation]

And finally, I am concerned about the target of Bill C-22. Indeed, we must always be mindful of the long-term impact of any legislation on the personal freedoms of all Canadians.

Consider, for instance, the potential for heightened citizen monitoring. By asking ISPs to intrude on the private communications of Canadians in order to uncover child pornography offences, would we be opening the door to widespread surveillance of law-abiding citizens?

And, in the absence of accountability and transparency, what happens to the innocent people whose private communications are misinterpreted by well-meaning but misdirected ISPs. The consequences for their lives and reputations can be incalculable.

In closing, Madam Chair, our office supports the efforts to combat the online sexual abuse of children with legislation that is targeted and effective.

The questions I am submitting to you are aimed at ensuring the effectiveness of Bill C-22, which, in our opinion, should be targeted at the actual guilty parties, and should be supported by accountability mechanisms that protect both children and the right to privacy in Canada.

I welcome your questions.

The Chair: Just before we go down the list, I have a question for you. Does the Personal Information Protection Act apply to the Internet service providers referred to in this bill?

Ms. Bernier: Yes.

The Chair: So you have a mandate?

Ms. Bernier: Absolutely, the act applies to them.

The Chair: You have the power to go and conduct investigations to determine whether everything is going as it should?

Ms. Bernier: Absolutely.

Senator Boisvenu: Thank you for submitting your brief. A word, it surprised me. I do not know whether we have the same reading of the bill. You obviously see it with different eyes from mine. I am more on the side of the victims, and you seem to be

En revanche, si la police reçoit un signalement — de la part d'un FSI, de Cyberaide ou de tout membre du public — relativement à du matériel suspect, un historique vérifiable est établi. La reddition de comptes devrait demeurer du ressort des autorités compétentes, c'est-à-dire, des organismes d'application de la loi. Il en va de l'intérêt des enfants et de celui de la société dans son ensemble.

[Français]

Finalement, je m'interroge sur le caractère ciblé du projet de loi C-22. En effet, nous devons toujours demeurer conscients des incidences à long terme de toute forme de législation sur les libertés personnelles de toutes les Canadiennes et de tous les Canadiens.

Prenons, par exemple, le potentiel d'intensification des mesures de surveillance des citoyens. En demandant aux FSI de s'immiscer dans les communications privées des Canadiennes et des Canadiens dans le but de lever le voile sur des infractions relatives à la pornographie juvénile, ouvrons-nous la porte à une surveillance généralisée des citoyens respectueux de la loi?

En l'absence de transparence et de mécanisme de reddition des comptes, qu'advient-il des personnes innocentes dont les communications privées sont mal interprétées par des FSI bien intentionnés mais mal orientés? Les conséquences éventuelles sur leur vie et leur réputation sont innombrables.

Pour conclure, madame la présidente, le Commissariat à la protection de la vie privée du Canada appuie les efforts pour combattre les abus pédosexuels en ligne au moyen d'une législation ciblée et efficace.

Les interrogations que je vous sou mets visent à assurer l'efficacité du projet de loi C-22 qui, à notre avis, exige une application ciblée aux véritables coupables, appuyé d'un mécanisme d'imputabilité qui protège à la fois les enfants et le droit à la vie privée au Canada.

Il me fera maintenant plaisir de répondre à vos questions.

La présidente : Juste avant de passer à la liste, j'aurais une question à vous poser. Est-ce que la Loi sur la protection des renseignements personnels s'applique aux fournisseurs de services Internet dont on parle dans ce projet de loi?

Mme Bernier : Oui.

La présidente : Donc, vous avez un mandat?

Mme Bernier : Absolument, la loi s'applique à eux.

La présidente : Vous avez le pouvoir d'aller faire des enquêtes pour vérifier si tout se passe comme il faut?

Mme Bernier : Tout à fait.

Le sénateur Boisvenu : Merci d'avoir déposé votre mémoire. Quelques mots dans celui-ci m'ont surpris. Je ne sais pas si nous faisons la même lecture du projet de loi. Évidemment, vous le faites avec des yeux différents des miens. Je suis plus du côté des

more on the side of caution. You talk about the word “policing”; you say we are going to delegate responsibility for policing to the ISPs. Did you see that word in the act?

Ms. Bernier: No, but that is in fact what we deduce from a reading of the bill. That is to say that, if you look at the second duty assigned to the ISPs, it is twofold. The first is that, when they receive a notice, they must report it and, second, when they themselves have reasonable grounds to believe that there is child pornography activity on their site, they must report it. It is in this second aspect that we necessarily expect them to exercise some diligence and thus some surveillance.

Senator Boisvenu: But do you not believe that the responsibility assigned them is more to denounce than to police? Obviously, when someone observes a violation of the act, an observation must be made, the information must be noted and then reported. But to take this definition in this document and say that we are going to assign responsibility for policing child pornography, do you not believe that you are going too far in your fear?

Ms. Bernier: If we had indeed read the bill as providing that the first duty of ISPs was to police child pornography, absolutely, I entirely agree with you. That would be an excessive extrapolation. However, what we note is that the bill leads the ISPs into a policing regime.

Senator Boisvenu: That is the question I want to ask you. I want you to show some caution. Where is it stated in the act that we are leading the ISPs into a pornography policing regime? Are we not leading them instead to keep a log of observations of breaches of the act and, when those people observe a breach of the act, they have a duty to report, not a duty to police?

Ms. Bernier: In fact, that is our reading of clause 3. In that clause, we see that the ISPs indeed have a responsibility to exercise a degree of diligence.

Senator Carignan: Good afternoon, Ms. Bernier; it is always a pleasure to welcome you. My question concerns the notion of mandate.

You said: “For that reason, I am concerned when I see that Bill C-22 obliges ISPs to seize and preserve all suspected computer data for 21 days, without a police request or a warrant.”

I do not see the warrant aspect very clearly; from what I understand of the bill, there is an obligation to report or to advise when the Internet service provider has reasonable or probable grounds to believe that its system or hosting site has been used to disseminate child pornography. It is being told, first, “You must report,” and, second, “You preserve must that data,” which is already on its computer. So we are not talking about seizing; we are talking about preserving.

victimes et vous semblez être plutôt du côté de la prudence. Vous parlez du mot « contrôler »; vous dite qu’on va déléguer une responsabilité de contrôle aux FSI. Est-ce que vous avez vu ce mot dans la loi?

Mme Bernier : Non, mais c’est en fait ce que nous déduisons de la lecture du projet de loi. C’est-à-dire que, si vous regardez la deuxième des obligations faites aux FSI, elle est double. La première est que, lorsqu’ils reçoivent un avis, ils doivent le communiquer et, deuxièmement, lorsqu’ils ont eux-mêmes des motifs raisonnables de croire qu’il y a une activité de pornographie juvénile sur leur site, ils doivent le rapporter. C’est dans ce deuxième aspect que, forcément, on s’attend à ce qu’ils devront exercer une certaine diligence, donc une certaine surveillance.

Le sénateur Boisvenu : Mais la responsabilité qu’on leur demande, ne croyez-vous pas que c’est plutôt de dénoncer plutôt que de contrôler? Évidemment, lorsqu’on observe une infraction à la loi, une observation doit être faite, un contrôle de l’information doit être fait, et ensuite une dénonciation. Mais prendre cette définition dans ce document et dire qu’on va donner la responsabilité de contrôler la pornographie juvénile, ne croyez-vous pas que vous allez trop loin dans votre crainte?

Mme Bernier : Si effectivement on avait lu le projet de loi comme étant une responsabilité première des FSI que de contrôler la pornographie juvénile, absolument, je suis tout à fait d’accord avec vous. Ce serait une extrapolation excessive. Cependant, ce que nous notons c’est que le projet de loi amène les FSI dans un régime de contrôle.

Le sénateur Boisvenu : C’est la question que je veux vous poser. Je veux que vous fassiez preuve de prudence. Où est-il écrit dans la loi qu’on amène les FSI à un régime de contrôle de la pornographie? Est-ce qu’on ne les amène pas plutôt dans un registre d’observation de manquement à la loi et, une fois que ces gens observent un manquement à la loi, ils ont l’obligation de dénoncer, et non l’obligation de contrôler?

Mme Bernier : En fait, c’est notre lecture de l’article 3. Nous voyons dans cet article une responsabilité pour les FSI, effectivement, d’exercer une certaine diligence.

Le sénateur Carignan : Bonjour, madame Bernier, c’est toujours un plaisir de vous accueillir. Ma question porte sur la notion de mandat.

Vous avez dit : « [...] toutes mes préoccupations à l’idée que le projet de loi C-22 oblige les FSI à saisir et à conserver toute donnée informatique suspecte pendant 21 jours, et ce, sans demande présentée par la police ni mandat ».

Je ne vois pas très bien l’aspect du mandat; à ce que je comprends du projet de loi, il y a une obligation de dénoncer ou d’aviser lorsque le fournisseur de services Internet a des motifs raisonnables et probables de croire que son système ou son site d’hébergement a été utilisé pour diffuser de la pornographie juvénile. On lui dit, premièrement, « tu dois dénoncer », et deuxièmement, « tu dois conserver ces données » qui sont déjà sur son ordinateur. Donc, on ne parle pas de saisir, on parle de conserver.

So for the person who has a contract, who decides to host child pornography material, that is the very nature of its service as an Internet service provider to host and preserve that information. So I find it hard to see how you can say that this becomes a seizure.

Second, this is an act by a private person. This is not an act of seizure by the state. So I find it hard to see the need for a warrant. That leads me to the other question; if you want to have warrants, the person who is informed, who is the police officer, must have reasonable and probable grounds to believe. So we have to have someone who gives that person the information; he studies it and subsequently goes and obtains a warrant to preserve that evidence, which is provided for under clause 4(2). He must preserve for 21 days and must destroy — I imagine that point must satisfy you.

Ms. Bernier: Absolutely.

Senator Carignan: Then it states: “. . . after the expiry of the 21-day period, unless the person is required to preserve the computer data by a judicial order or under any other Act of Parliament or the legislature of a province.” That assumes, at that point, that someone — I imagine the state or a representative of the state — has acquired a preservation order, which is a form of warrant. Is your suggestion of a warrant or seizure by the Internet service provider that reports not a bit premature? Is that not putting the cart before the horse?

Ms. Bernier: First of all, I want to emphasize something you yourself have raised, and that is that there are indeed provisions in the bill that we consider highly respectful of the protection of personal information and privacy, such as the obligation to destroy 21 days later — the act clearly states “immediately after 21 days.” We hail this as entirely appropriate. The point where we have, not a fear, but rather a wish to invite you to consider it is that, in clause 4, preservation, which is usually done in accordance with a preservation order, would be done without a preservation order and, as you can see in the wording, refers to any kind of information. It clearly states: “must preserve all computer data related to the notification that is in their possession or control for 21 days.”

There we have information that is preserved for 21 days and that could be entirely harmless. So it is quite broad, and this preservation is done in the absence of any request by the police or a judge. It is simply what we want to highlight, that there is a certain latitude in this duty to preserve.

Senator Carignan: The information may be harmless, but it nevertheless states that the Internet service provider must have reasonable and probable grounds to believe that it is related to the dissemination of child pornography. So the information may seem harmless to the uninitiated, but is extremely useful for the police department in looking for the person who has committed this offence or who has taken the picture.

Donc pour la personne qui a un contrat, qui a décidé d'héberger du matériel de pornographie juvénile, c'est la nature même de son service de fournisseur de services Internet que d'héberger et de conserver cette information. Donc, j'ai de la misère à voir comment vous pouvez dire que cela devient une saisie?

Deuxièmement, c'est un acte d'une personne privée. Ce n'est pas un acte de saisie de l'État. Donc, je vois mal la nécessité d'un mandat. Cela m'amène à l'autre question; si vous voulez avoir des mandats, la personne qui est informée, qui est l'agent de police, doit avoir des motifs raisonnables et probables de croire. Donc on doit avoir quelqu'un qui lui donne cette information, il l'étudie et, par la suite, il va aller chercher un mandat pour conserver cette preuve, ce qui est à l'article 4(2). Il doit conserver pendant 21 jours et doit détruire — j'imagine que ce point doit vous satisfaire.

Mme Bernier : Absolument.

Le sénateur Carignan : On dit ensuite : « [...] après l'expiration des 21 jours, à moins qu'elle ne soit assujettie à une ordonnance de préservation rendue en vertu d'une autre loi fédérale ou provinciale à l'égard de ces données ». Cela présume, à ce moment, que quelqu'un, j'imagine l'État ou un représentant de l'État, a eu une ordonnance de conservation, donc une forme de mandat. Est-ce que votre suggestion de mandat ou de saisie au niveau du fournisseur de services Internet qui dénonce n'est pas un peu prématurée? Est-ce que ce n'est pas mettre la charrue avant les bœufs?

Mme Bernier : Je veux souligner tout d'abord ce que vous avez-vous-même soulevé, c'est que, effectivement, il y a des dispositions dans le projet de loi qui nous paraissent très respectueuses de la protection des renseignements personnels et de la vie privée, par exemple l'obligation de détruire 21 jours après — la loi dit bien « immédiatement après 21 jours ». Nous le saluons comme étant tout à fait approprié. Le point pour lequel nous aurions, non pas une crainte, mais plutôt le souhait de vous inviter à le considérer, c'est que, à l'article 4, la préservation, qui habituellement se fait selon un ordre de préservation, se ferait, justement, sans ordre de préservation, et, comme vous pouvez le noter dans le libellé, se rapporte à n'importe quelle information. Cela dit bien : « préserve les données informatiques afférentes en sa possession ou à sa disposition pendant 21 jours ».

On a là de l'information qui est gardée pendant 21 jours et qui pourraient être tout à fait anodine. C'est donc assez large, et cette préservation se fait en l'absence de toute demande de la police ou d'un juge. C'est simplement ce que nous voulons mettre en lumière, qu'il y a une certaine largesse dans cette obligation de préservation.

Le sénateur Carignan : L'information peut être anodine, mais on dit quand même que le fournisseur de services Internet doit avoir des motifs raisonnables et probables de croire que c'est relié à la diffusion de pornographie juvénile. Donc, l'information peut sembler anodine pour un profane, mais extrêmement utile pour le service de police pour rechercher la personne qui a commis cette infraction ou qui a pris la photo.

Ms. Bernier: Absolutely. But that relates to our other argument, which was: will all ISPs be able to conduct this analysis of reasonable grounds to believe? So, if we start from the assumption that not all ISPs will be able to apply this notion, we may therefore fear a slight deviation from clause 4, because they would preserve information that is not consistent with the spirit of clause 3.

Senator Carignan: What are you proposing to improve privacy protection and to be effective enough so that we do not bog down in bureaucracy?

Ms. Bernier: We recently read the RCMP's testimony on this subject. We also read the reports on the effectiveness of CyberTip. We realize that there is currently a good system whereby people inform, where that information is reported to the competent authorities, who enforce the law.

We find that the current process is effective in combating child pornography while respecting privacy and being very targeted in its application.

Senator Carignan: Do you not think that the fact that it is not validated by a statutory provision that would give it a legal basis might be considered an abuse? Would it not be preferable to have a legislative support to provide a framework for this practice?

Ms. Bernier: Absolutely. That is why I began my remarks by telling you how pleased we are to see that the government has established legislation and is developing it.

I also remind you of the resolution our commissioner sponsored in 2008 calling precisely for legislation to provide this statutory support you are referring to.

[English]

Senator Runciman: When were you asked to appear before the committee and comment on this legislation?

Ms. Bernier: I believe it was last Friday.

Senator Runciman: I have suspicions about the amount of time spent taking a look at the implications of the legislation. You referenced the 21-day period as an example, and I know Senator Carignan spoke to that issue. Police have told the government and others that is a reasonable period of time to obtain a judicial order for further preservation or production of the data, and in some cases to obtain a search warrant. That is what the 21 days is all about.

I know you have criticized the 21 days. They require that time if someone does suspect something has happened. They are asked to preserve that data for that period of time to allow the authorities to do what they have to do to pursue it, if they believe it has merit in terms of further investigation.

Mme Bernier : Tout à fait. Mais voilà, cela se rapporte à notre autre argument qui était : est-ce que tous les FSI vont être en mesure de bien exercer cette analyse de motif raisonnable de croire? Alors, si on part de la prémisse que ce n'est pas tous les FSI qui vont être en mesure de bien appliquer cette notion, on peut donc craindre un petit dérapage à l'article 4, parce qu'effectivement ils préserveraient de l'information qui ne correspond pas à l'esprit de l'article 3.

Le sénateur Carignan : Que proposez-vous pour améliorer la protection de la vie privée et pour être assez efficace qu'on ne s'enfarge pas dans la bureaucratie?

Mme Bernier : On a lu évidemment les témoignages de la GRC à ce sujet. On a lu également les rapports sur l'efficacité de Cyberaide. On se rend compte qu'en ce moment il y a un bon système par lequel les gens dénoncent, où ces dénonciations sont rapportées aux autorités compétentes, qui elles appliquent la loi.

Nous trouvons que le processus actuel est efficace pour contrer la pornographie infantile tout en respectant la vie privée et en étant très ciblé dans son application.

Le sénateur Carignan : Le fait qu'il ne soit pas validé par une disposition législative qui le soutiendrait juridiquement, pensez-vous que cela peut être considéré comme abusif? N'est-il pas préférable d'avoir un support législatif pour encadrer cette pratique?

Mme Bernier : Absolument. C'est pour cela que j'ai commencé mes remarques en vous disant à quel point nous sommes heureux de voir que le gouvernement a mis sur pied de la législation et qu'il est en train de la développer.

Je vous rappelle également la résolution que notre commissaire a parrainé en 2008, qui demande précisément de la législation pour donner cet appui statutaire auquel vous faites référence.

[Traduction]

Le sénateur Runciman : Quand vous a-t-on demandé de comparaître devant le comité et de présenter des commentaires au sujet de ce projet de loi?

Mme Bernier : Je pense que c'était vendredi dernier.

Le sénateur Runciman : J'entretiens quelques doutes au sujet du temps que vous avez consacré à l'examen des répercussions de ce projet de loi. Vous avez donné comme exemple la période de 21 jours et je sais que le sénateur Carignan a parlé de cet aspect. Les services de police ont dit au gouvernement et à d'autres que cela représentait une période d'une durée raisonnable pour obtenir une ordonnance judiciaire de préservation et de communication des données; et pour dans certains cas, obtenir un mandat de perquisition. C'est là le contexte de cette période de 21 jours.

Je sais que vous l'avez critiqué. Ils ont besoin de disposer de ce temps lorsque quelqu'un soupçonne que quelque chose a été commis. On leur demande de préserver les données pendant cette période pour que les autorités prennent les mesures qui s'imposent, si elles estiment qu'il y a lieu d'approfondir une enquête.

You talked about privacy, as well. Clause 5 speaks to that, as does clause 6, in my view. They state a person must not disclose; they have made a report. Although the government is taking the position that clause 6 was placed in the bill to not give a defence to someone who might say they were simply pursuing their suspicions, there is also a privacy element contained in that as well. Therefore, I think that has been a concern and consideration of the government.

You reference expertise in your submission about ISPs — do they have the necessary expertise to enforce the law? I do not think they are being called upon by anything in this legislation to enforce the law, the way I interpret it. I think they are asking others who have those responsibilities, if there is a merit to the concerns, to carry out the responsibilities to enforce the law. I do not think any private citizen or any company provider is being asked to enforce the law. I had some difficulty with that suggestion, as well.

Your third question talked about accountability and not defining exactly what information the ISP must preserve. They can preserve anything from anyone without the knowledge of the owners of the information and without judicial oversight. Again, that deals with the 21-day period. Perhaps I am misinterpreting you or not being fair to you in terms of the way I am interpreting your position on this, but you seem to be of the opinion that the child's rights are outweighed by the rights of the customer who might be participating in the production or the distribution of this very offensive and harmful material.

I have a lot of difficulty with the position you have put forward here today. I think this is outstanding legislation, and you talk about the need for it. I think you also imply that Cybertip, for example, is perhaps not trustworthy with respect to dealing with these kinds of concerns, initially. Again, I have trouble with that.

The Chair: Is there a question?

Senator Runciman: I think these are concerns being expressed and the witness will have an opportunity to respond.

There is one other, but you have thrown me off my line of thought here, Madam Chair. Maybe I will come back to it. We will let the witness respond if she wishes.

Ms. Bernier: Certainly. I do not believe we are nearly as far apart as you may have been given the impression of. We came here to bring to you some questions to consider to make this piece of legislation even better.

First, if I gave the impression that we thought Cybertip was not trustworthy, it is exactly the opposite. We feel they are doing an excellent job and they should be the partner with law enforcement

Vous avez également parlé de vie privée. L'article 5 en parle, tout comme l'article 6, à mon avis. Ces articles disent que le fournisseur ne doit pas révéler avoir fait un signalement. Le gouvernement affirme que l'article 6 a été ajouté au projet de loi pour que quelqu'un ne puisse invoquer en défense le fait qu'il ne faisait que vérifier des soupçons, mais cette disposition contient également un élément protégeant la vie privée. C'est pourquoi je pense que c'est là une préoccupation du gouvernement et un élément dont il a tenu compte.

Vous faites référence à l'expertise dans votre mémoire au sujet des FSI — ces derniers possèdent-ils l'expertise nécessaire pour appliquer la loi? Je ne pense pas que le projet de loi leur demande d'appliquer la loi, d'après ce que je comprends. Je pense qu'ils demandent à ceux qui ont ces responsabilités de vérifier le bien-fondé de leurs préoccupations, d'exercer leurs responsabilités en matière d'application de la loi. Je ne pense pas que l'on demande à un citoyen ou à une société qui fournit des services d'appliquer la loi. Je me suis aussi posé quelques questions au sujet de cette suggestion.

Votre troisième question portait sur la reddition de comptes et sur le fait que l'on ne définissait pas exactement le genre de renseignements que les FSI doivent préserver. Ils peuvent préserver tout ce qu'ils veulent sur tout le monde sans la connaissance des propriétaires de l'information et sans contrôle judiciaire. Là encore, cela concerne la période de 21 jours. Il est possible que je vous interprète mal ou que je n'interprète pas votre position de façon équitable, mais vous semblez penser que les droits de l'enfant doivent céder le pas aux droits du client qui est peut-être en train de produire ou de distribuer un matériel particulièrement choquant et nuisible.

J'ai beaucoup de mal à accepter la position que vous avez présentée aujourd'hui. Je pense que nous avons là un excellent projet de loi et vous dites que nous en avons besoin. Je crois que vous laissez également entendre qu'il ne serait peut-être pas souhaitable de confier à Cyberaide ce genre de chose, parce que cet organisme ne serait pas digne de confiance. Encore une fois, j'ai du mal à accepter ce commentaire.

La présidente : Allez-vous poser une question?

Le sénateur Runciman : Ce sont là les préoccupations que j'ai exprimées et le témoin aura la possibilité d'y répondre.

Il y en avait une autre, mais vous m'avez troublé, madame la présidente. J'y reviendrai peut-être plus tard. Nous allons laisser le témoin répondre à mes commentaires si elle le souhaite.

Mme Bernier : Certainement. Je ne pense pas que nos positions soient aussi éloignées l'une de l'autre que vous le pensez. Nous sommes venues ici pour poser quelques questions visant à améliorer encore ce projet de loi.

Premièrement, si j'ai donné l'impression que nous ne pensions pas que Cyberaide était digne de confiance, je me suis mal exprimée, parce que c'est exactement le contraire. Nous estimons

to continue. We have every reason to believe they are trustworthy. I may have misspoken and I apologize if that was the case. Let me correct the record.

In relation to the 21 days, the issue is that preservation is usually done with a preservation order, and you can get a preservation order more quickly than 21 days. You may want to check this again, but this has to be verified with operational needs. However, judges are available 24-7 and can respond quickly. Therefore, perhaps looking at whether the 21 days is a necessary time is an avenue that could be pursued by this committee.

The Chair: I have a supplementary. Is your problem that 21 days is too short, too long, or is it the absence of a judicial order?

Ms. Bernier: It is the absence of a judicial order that comes and verifies the reasons for having preserved information.

Senator Runciman: I should put on the record that the 21-day period is consistent with amendments relating to the preservation command and order contained in Bill C-51, An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act. Therefore, this is something that has been discussed at length with policing officials and others who have interest in these areas. To some degree, it has been described as a reasonable compromise in that it meets the needs of the police and reflects the realities of the providers of Internet services.

You also talked about the system working well with individual citizens calling in. We have heard, and there has been testimony to this effect, that 30 per cent to 40 per cent of the ISPs have, in the past, refused to cooperate with police. I think a lack of cooperation from a significant number of providers is what has driven this legislation. The status quo in terms of direct reporting through Cybertip or to a policing agency has been a weakness that the government is trying to address.

Ms. Bernier: We, too, are very concerned about the fact that there are ISPs who refuse to cooperate, and that is one of the reasons we welcome legislation.

[Translation]

Senator Chaput: You said you currently had a good reporting system and a process that complies with private law. Were you talking about a partnership with police officers?

que cet organisme fait de l'excellent travail et que son association avec les services d'application de la loi devrait se poursuivre. Nous avons tous raison de croire que c'est un organisme digne de confiance. Je me suis peut-être mal exprimée et je vous prie de m'en excuser si c'est le cas. Je souhaiterais corriger le compte rendu.

Pour ce qui est de la période de 21 jours, la question découle du fait que la préservation découle habituellement d'une ordonnance de préservation et qu'il est possible d'obtenir ce genre d'ordonnance en moins de 21 jours. Vous voudrez peut-être vérifier ce point à nouveau, mais il faut que cela soit conforme aux besoins opérationnels. Il est possible d'avoir accès à un juge 24 heures par jour, sept jours par semaine, et il peut répondre rapidement. C'est la raison pour laquelle le comité voudra peut-être continuer à examiner la question de savoir si une période de 21 jours est vraiment nécessaire.

La présidente : J'ai une question supplémentaire. Le problème que vous soulevez vient-il du fait qu'une période de 21 jours est trop courte, trop longue ou est-ce l'absence d'une ordonnance judiciaire?

Mme Bernier : C'est l'absence d'une ordonnance judiciaire ayant pour but de vérifier les motifs pour lesquels ces renseignements sont préservés.

Le sénateur Runciman : Je devrais mentionner pour le compte rendu que la période de 21 jours est conforme aux amendements concernant l'ordonnance de préservation et l'ordonnance visée par le projet de loi C-51, Loi modifiant le Code criminel, la Loi sur la concurrence et la Loi sur l'entraide juridique en matière criminelle. C'est donc un aspect qui a été abordé en détail avec les représentants des services de police et des autres services qui s'intéressent à ces questions. Cette période a, dans l'ensemble, été décrite comme proposant un compromis raisonnable dans le sens qu'elle répond aux besoins de la police et tient compte de la situation réelle des fournisseurs de services Internet.

Vous avez également dit que le système fonctionnait très bien parce qu'il confiait aux citoyens le soin de signaler ce genre de chose. On nous a dit, et nous avons reçu des témoignages à cet effet, que 30 à 40 p. 100 des FSI ont déjà refusé de collaborer avec la police. Je crois que c'est le manque de collaboration de la part d'un bon nombre de fournisseurs de services qui est à l'origine de ce projet de loi. Le statu quo pour ce qui est des signalements directs à Cyberaide ou à un service de police n'est pas satisfaisant et constitue une faiblesse à laquelle le gouvernement essaie de remédier.

Mme Bernier : Nous sommes également très préoccupés par le fait qu'il y a des FSI qui refusent de collaborer et c'est une des raisons pour lesquelles nous appuyons ce projet de loi.

[Français]

Le sénateur Chaput : Vous avez dit que vous aviez présentement un bon système de dénonciation et un processus qui respecte la loi privée. Parlez-vous d'un partenariat avec les agents de police?

Ms. Bernier: I was referring to the present structure in which Cybertip receives reports and forwards them to the police departments.

The police departments intervene very often, if necessary immediately, on an ad hoc basis. There is a protocol with most ISPs. Our concern, as Senator Runciman said, is indeed that not everyone is cooperating. However, we feel that, if we can guarantee full cooperation, the present system seems to operate well and its value is that it does not result in the even broader dissemination of these photographs of children, which are exactly the way to make them victims.

Senator Chaput: Does this bill help ensure a better system for reporting that also respects privacy? I am going beyond privacy because, in my opinion, children are never guilty; they are always victims. Their privacy is taken away before they even have it.

Is it your concern that the bill does not adequately respect privacy, or is it that it does not do enough to protect children?

Ms. Bernier: With respect to children's privacy, the fact that even more stakeholders are being added concerns us in that there is this potential for broader exposure of children. This is precisely how children become victims in child pornography; it is by this exposure. So we think that increasing the number of stakeholders is a concern in relation to respect for children's privacy and integrity. We also wonder whether this will be more effective. Is it really effective to have so many stakeholders or is it not more effective now to combat child pornography in a very targeted manner?

That said, as I said in response to Senator Carignan, there are provisions in the act, and Senator Runciman said this as well, that respect privacy, that clearly stem from a concern to respect privacy, and we recognize that.

[English]

Senator Munson: In your estimation, would it make more sense to have the Internet service provider simply report directly to the police? As the opposition critic in the Senate, I note that there are a couple of reporting mechanisms here. Would it make more sense to exclude the other and just have it done to the police who are mandated to investigate and make possible arrests?

Ms. Bernier: Do you mean rather than going through the designated body?

Senator Munson: Yes, I do.

Ms. Bernier: That is interesting. Yes, I suppose that would ensure that you have a direct line that would go directly to the competent authorities who could immediately make a good judgment as to whether this indeed should be taken further.

Mme Bernier : Je faisais référence à la structure actuelle, où Cyberaide reçoit les dénonciations puis les transmet aux services de police.

Les services de police interviennent très souvent, si c'est nécessaire de façon immédiate, ponctuelle. Il y a un protocole avec la plupart des FSI. Notre préoccupation effectivement, comme le disait le sénateur Runciman, c'est que tous ne collaborent pas. Mais nous trouvons que si on peut assurer une collaboration complète, ce système actuel semble bien fonctionner et à cette valeur qu'il n'encourt pas la diffusion encore plus large de ces photos d'enfants qui sont exactement la façon de les rendre victimes.

Le sénateur Chaput : Ce projet de loi contribue-t-il à assurer un meilleur système qui dénonce et aussi qui respecte la vie privée. Je vais plus loin que la vie privée parce que, à mon avis, l'enfant n'est jamais coupable, il est toujours victime. On lui enlève sa vie privée avant même qu'il en ait une.

Est-ce votre inquiétude que le projet de loi ne respecte pas suffisamment la vie privée ou est-ce que c'est parce qu'il ne contribue pas suffisamment à protéger l'enfant?

Mme Bernier : Pour ce qui est de la vie privée de l'enfant, le fait qu'on ajoute encore des intervenants nous préoccupe en ce sens qu'il y a ce potentiel d'exposition élargie de l'enfant. C'est justement ainsi que l'enfant devient victime dans la pornographie infantile, c'est par cette exposition. Donc, de voir cet élargissement des intervenants, cela nous préoccupe par rapport au respect de la vie privée de l'enfant, de son intégrité. On se demande aussi si cela va être plus efficace. Est-ce vraiment efficace d'avoir tant d'intervenants ou si ce n'est pas plus efficace maintenant d'avoir une façon très ciblée d'arriver de combattre la pornographie juvénile?

Ceci étant dit, comme je l'ai dit en réponse au sénateur Carignan, il y a des dispositions dans la loi, et le sénateur Runciman l'a dit aussi, qui sont respectueuses de la vie privée, qui clairement émanent d'un souci de respect de la vie privée, et nous le reconnaissons.

[Traduction]

Le sénateur Munson : À votre avis, serait-il plus logique de demander aux fournisseurs de services Internet de signaler ce genre de chose directement à la police? En tant que porte-parole de l'opposition au Sénat, je remarque qu'il existe déjà quelques mécanismes de signalement. Serait-il plus logique d'exclure l'autre et de signaler les cas uniquement à la police qui a pour rôle de faire enquête et éventuellement de procéder à des arrestations?

Mme Bernier : Vous voulez dire plutôt que de s'adresser à un organisme désigné?

Le sénateur Munson : Oui.

Mme Bernier : Voilà qui est intéressant. Oui, je suppose qu'il y aurait de cette façon une ligne directe qui rejoindrait directement les autorités compétentes, qui pourraient alors immédiatement décider s'il y a lieu d'aller plus loin.

That being said, I would be reluctant to give you a specific or prescriptive manner to improve, other than to say we would ensure that we streamline the number of intervenors as much as possible, and that we would subject the reporting to a very robust accountability mechanism.

Senator Munson: What does that mean?

Ms. Bernier: It means, for example, making sure that the reporting goes straight to a competent authority, including law enforcement; that there is an audit trail; that there is, as in the bill, a duty to destroy as soon as the evidence is no longer necessary, and so forth.

Senator Munson: You also say in your statement that the bill would make cyber cafés, hotels, mom-and-pop restaurants and public libraries responsible for policing child pornography. Could you elaborate a little on that? I am trying to envisage that picture. In the world we live in today, they are there by the hundreds of thousands. Sometimes I have that perception of Big Brother looking over your shoulder. You are using a cyber-café Internet service provider and up pops something that is horrible that no one ever wants to see. At that point, how does this all move into action? Is it reported to the police from something as simple as that, when it could be a very innocent look at a particular website that some people may find offensive, and that people see in our society today?

Ms. Bernier: That is our understanding of the House of Commons debates so far — that, indeed, that is the intent. It would cover any ISP, and it would mean anyone who would offer the infrastructure and host a site. We would infer from that that it would include even mom-and-pop — fairly unsophisticated, if I can say so — ISP providers or entrepreneurs who would then apply the act, perhaps not with all the knowledge that would be necessary to apply it well and, therefore, perhaps undermine its efficiency rather than enhance it.

Senator Munson: That is a heavy responsibility for these folks, in the world we live in.

Ms. Bernier: It would be highly regrettable should the law enforcement authorities be so burdened by irrelevant information that they would not actually get at the true guilty.

Senator Munson: I have notes here in front of me that state if a person reports a child pornography offence to the authorities, that person may be asked to testify in court. Should the identity of those persons who assist the authorities in uncovering the abuse of children be protected, as they are in the United Kingdom?

Cela dit, j'hésiterais à vous proposer une manière précise ou obligatoire d'améliorer cet aspect, sinon que de dire qu'il conviendrait de limiter le plus possible le nombre des intervenants et d'associer les signalements à un mécanisme de reddition de comptes qui serait très strict.

Le sénateur Munson : Que voulez-vous dire?

Mme Bernier : Cela veut dire, par exemple, veiller à ce que le signalement se rende directement à l'autorité compétente, y compris au service d'application de la loi, qu'il y ait un document de vérification et qu'on prévoie, tout comme le projet de loi, l'obligation de détruire les éléments de preuve dès qu'ils ne sont plus nécessaires, par exemple.

Le sénateur Munson : Vous avez également dit dans votre exposé qu'avec le projet de loi, les cybercafés, les hôtels, les restaurants familiaux et les bibliothèques publiques seraient chargés de réprimer la pornographie juvénile. Pourriez-vous préciser un peu cela? J'essaie d'imaginer la situation. Dans le monde dans lequel nous vivons aujourd'hui, il y en a des centaines de milliers. J'ai parfois l'impression que Big Brother est derrière moi et me surveille. Vous utilisez l'accès Internet d'un cybercafé et, tout à coup, vous voyez quelque chose d'horrible que personne ne voudrait voir. À ce moment-là, comment passe-t-on à l'action? Faut-il signaler cette situation à la police après avoir fait une constatation aussi simple que celle-ci, alors qu'il pourrait s'agir d'un regard très innocent porté sur un site web particulier que certaines personnes trouvent choquant, mais que les gens voient couramment dans notre société?

Mme Bernier : C'est ce que nous avons retenu des débats qui ont eu lieu jusqu'ici devant la Chambre des communes — que c'est bien là l'intention. Le projet de loi viserait n'importe quel FSI, et cela veut dire toute personne qui offre une infrastructure et héberge un site. Nous en déduisons que cela engloberait les entreprises familiales — même si elles sont généralement peu sophistiquées — qui fournissent des services Internet ou des entrepreneurs qui appliqueraient ensuite la loi, peut-être sans avoir toutes les connaissances qui seraient nécessaires pour bien le faire et par conséquent, compromettrait l'efficacité du projet de loi plutôt que la renforcer.

Le sénateur Munson : C'est une lourde responsabilité que nous imposons à ces personnes, dans notre monde d'aujourd'hui.

Mme Bernier : Il serait extrêmement regrettable que les responsables de l'application de la loi reçoivent tellement de renseignements inutiles que cela les empêche de trouver les véritables coupables.

Le sénateur Munson : J'ai des notes devant moi qui mentionnent que, si une personne signale une infraction relative à la pornographie juvénile aux autorités, cette personne peut être amenée à témoigner devant le tribunal. Est-ce que l'identité des personnes qui aident les autorités à détecter l'exploitation des enfants devrait être confidentielle, comme c'est le cas au Royaume-Uni?

Ms. Bernier: Obviously, as an officer who is mandated to protect privacy, we would say yes, because that would be a situation where revealing identity could cause harm. Spontaneously, I would say that it could certainly be a very valid measure.

Senator Munson: There is one other point here in some of the questions from our great researchers. Some of what we do is spontaneous, but there are other questions here.

I do not know if you can answer this, but is Canada Post committing an offence if someone sends child pornography through the mail, and it is known to Canada Post but it does nothing about it, or is Bell Canada committing an offence in similar circumstances — in your estimation?

Ms. Bernier: That is a criminal law question. I would not answer that. Sorry, I do not feel it is appropriate for me to answer that.

Senator Munson: We can ask other witnesses that question.

[Translation]

Senator Joyal: I have two points. The first concerns what you contend on page 4 of your brief. Based on your experience, there is a risk of “over-reporting” on the basis that now, since there is an offence, Internet service providers will prefer to take the risk of reporting everything rather than determine themselves whether there are situations of child pornography because you say they are not equipped to rule or make a judgment on the nature of the site in question.

And I link that to a statement that we received from the ombudsman for victims, whom we heard in this committee last week, where she said:

[English]

Furthermore, while this proposed legislation will most likely help law enforcement to identify further leads, it will not address the current backlogs that many law enforcement agencies face in investigating these cases, due to a lack of resources and staffing.

[Translation]

If I understand you, your concern is similar to that of the federal ombudsman for victims, that this in a way causes an increase in the number of reports. Considering as well the testimony that we have heard from police officers, who say they cannot proceed within 21 days in a number of cases, and as the bill requires the information to be destroyed after 21 days, in principle, we are creating the expectation that the system will be more effective.

Mme Bernier : Évidemment, en tant qu'autorité chargée de protéger la vie privée, nous dirions que oui, parce que, dans cette situation, la divulgation de l'identité pourrait causer un préjudice. Spontanément, je dirais que cela pourrait certainement être une mesure très positive.

Le sénateur Munson : Il y a un autre aspect qui est mentionné dans les questions proposées par nos grands chercheurs. Certaines de nos questions sont spontanées, mais il y a d'autres questions ici.

Je ne sais pas si vous pouvez répondre à cette question, mais j'aimerais savoir si Postes Canada commet une infraction lorsqu'une personne envoie de la pornographie juvénile par courrier et que Postes Canada le sait, mais n'intervient pas, ou est-ce que Bell Canada commet une infraction dans des circonstances semblables — à votre avis?

Mme Bernier : C'est une question de droit pénal. Je ne suis pas en mesure de vous répondre. Désolée, je ne pense pas qu'il soit approprié que je réponde à cette question.

Le sénateur Munson : Nous pourrions poser la question à d'autres témoins.

[Français]

Le sénateur Joyal : Deux points, le premier, au sujet de ce que vous soutenez à la page 4 de votre mémoire. Selon votre expérience, il y a un risque de « surdéclaration » sur la base que maintenant, étant donné qu'il s'agit d'une infraction, les fournisseurs de services Internet vont préférer plutôt prendre le risque de tout déclarer plutôt que de juger eux-mêmes les situations de pornographie juvénile ou non, parce que vous dites qu'ils ne sont pas outillés pour se prononcer ou porter un jugement sur la nature du site en question.

Et je relie cela à une déclaration que nous avons reçue de l'ombudsman des victimes, que nous avons entendu à ce comité la semaine dernière, où elle dit ceci :

[Traduction]

En outre, le projet de loi va certes très probablement aider les services d'application de la loi à trouver d'autres pistes, mais il ne va pas réduire l'arriéré actuel qu'ont de nombreuses agences d'application de la loi dans les enquêtes sur ce genre d'affaires, parce qu'elles manquent de ressources et de personnel.

[Français]

Si je comprends, votre préoccupation rejoint celle de l'ombudsman fédéral des victimes voulant que cela provoque, d'une certaine façon, une multiplication du nombre des déclarations. Compte tenu également des témoignages que nous avons entendus des policiers selon lesquels qu'on ne peut procéder à l'intérieur de 21 jours dans plusieurs cas, et comme le projet de loi oblige la destruction de l'information après 21 jours, en

However, in your assessment, you doubt that the actual impact of this bill will be a greater ability to take individuals guilty of using child pornography on Internet sites to court?

Ms. Bernier: That comment is based on our experience, as I said in my remarks on FINTRAC. We have seen excessive reporting, in which utterly harmless transactions were reported out of caution. People report everything in order to be sure they are meeting their obligations.

Exactly as you say, and as you have been told by other witnesses, this impedes the competent authorities. They are so submerged under information that it is very hard or takes a very long time to tell the relevant information from the irrelevant. As a result, instead of helping them, we hurt them.

That is why I emphasized the targeted nature of the information in my remarks. We would like to ensure that the act permits highly targeted intervention and thus genuinely helps the competent authorities by providing relevant information.

Senator Joyal: I am going back to your brief, where you say that accountability should remain where it belongs, namely with law enforcement agencies, and that this best serves the interests of children and society as a whole.

Do you mean that, by going through Internet service providers, we are complicating the process and that we are not only complicating it, but, in practice, we are putting the protection of privacy at greater risk? Should people not make their reports to police?

Ms. Bernier: There is indeed a risk that we will complicate it if the ISPs behave like the other institutions that we now see put at the service of law enforcement officers, like for FINTRAC, banking institutions, casinos and other institutions, whose natural inclination is to report more information in order to meet their legal obligations.

We can expect that the ISPs will do the same. That is where we fear there will be such a deluge of information that the public security agencies will be even less well equipped to address actual incidents than they are now.

Senator Joyal: Do you think the 21-day time period is too long, or do you think the duty under clause 4 to destroy information from the site after 21 days does not adequately protect privacy?

Ms. Bernier: On the contrary. The duty to destroy very clearly stems from a proper concern to protect privacy. However, I suggest you consider the fact that there is a provision requiring the ISPs to immediately obtain a preservation order if they genuinely believe there are reasons to do so.

principe, on crée l'expectative que le système va être plus efficace. Cependant, votre évaluation est de douter de l'impact réel de ce projet de loi quant à la capacité de mener devant les tribunaux les personnes coupables d'utiliser la pornographie juvénile sur des sites Internet?

Mme Bernier : Cette remarque est fondée sur notre expérience, comme je le disais dans mes remarques sur le CANAFE. On a vu un rapport excessif, où des transactions tout à fait anodines étaient dénoncées par prudence. On dénonce tout pour être sûr qu'on remplit nos obligations.

Exactement comme vous le dites et comme vous vous l'êtes fait dire par d'autres témoins, cela crée un embourbement des autorités compétentes. Ils sont submergés d'informations à un point tel qu'il soit très difficile ou très long de discerner l'information pertinente de l'information non pertinente. Cela a pour résultat qu'au lieu de les aider on leur nuit.

C'est pour cela que j'ai insisté dans mes remarques sur le caractère ciblé de l'information. On voudrait s'assurer que la loi permette une intervention très ciblée et aide donc véritablement les autorités compétentes avec de l'information pertinente.

Le sénateur Joyal : Je reviens à votre mémoire où vous dites que la reddition de compte devrait demeurer du ressort des autorités compétentes, c'est-à-dire des organismes d'application de la loi, et qu'il en va de l'intérêt des enfants et de celui de la société dans son ensemble.

Est-ce que vous voulez dire qu'en passant par le biais des fournisseurs de services Internet on alourdit le processus, et que non seulement on l'alourdit mais qu'en pratique on fait en sorte que la protection de la liberté privée s'en trouvera davantage à risque. Ne devrait-on pas faire la déclaration à la police?

Mme Bernier : On risque de l'alourdir effectivement si les FSI se comportent comme les autres institutions que l'on voit maintenant mises au service des agents de protection de la loi, comme pour le CANAFE, les institutions bancaires, les casinos, et autres, qui ont le réflexe naturel de transmettre plus d'informations pour satisfaire leurs obligations juridiques.

On peut s'attendre à ce que les FSI fassent la même chose. C'est là qu'on craint qu'il y ait justement un tel déluge d'informations que les agences de sécurité publique seront encore moins bien outillées pour répondre aux véritables incidents qu'ils ne le sont maintenant.

Le sénateur Joyal : Trouvez-vous que le délai de 21 jours est trop long ou trouvez-vous que l'obligation faite à l'article 4 de détruire après 21 jours les informations du site ne protège pas suffisamment la vie privée?

Mme Bernier : Au contraire. L'obligation de destruction émane de façon claire d'une juste préoccupation pour la protection de la vie privée. Cependant, je vous suggère de considérer qu'il y ait une disposition qui demande au FSI d'obtenir immédiatement un ordre de préservation s'ils considèrent véritablement qu'il y a matière.

We are not necessarily saying that the 21-day time period is too long, but we would like data preservation to be subject to an accountability mechanism such as a judicial authorization, for example.

Senator Joyal: You are suggesting an intermediate stage between what we currently have in the bill and what you are proposing, that when a service provider is notified by a person that its site is being used to disseminate child pornography, the provider immediately go to court to get a preservation order.

Ms. Bernier: It is not the service provider that would do that, but it could immediately contact police, who could intervene and obtain a preservation order. If it were provided with a better framework, we believe, we hope, and this is subject to consideration and deliberation with other expert witnesses, that this would streamline the process so that we would gather only relevant information and target only guilty parties. So we would better equip the security agencies to intervene.

Senator Joyal: Would you like to see an additional process provided for in the bill?

Ms. Bernier: For example, from the moment the ISP observes that its site has been used to spread child pornography and immediately reports that fact to the security agencies which will obtain a preservation order and use the information in order to take action.

Senator Joyal: You know that some cases may very obviously involve child pornography but that others may be less clear. We risk finding ourselves in the situation we were criticizing earlier, where, to avoid breaking the law, people report virtually everything. This is where the bill contains an additional problem that will not facilitate the fight against child pornography. We are going to give ourselves good intentions, but the bill lacks mechanisms to make it effective. Other witnesses have suggested this to us, and I believe it is an extremely important factor that we should consider in our discussions on this bill.

Ms. Bernier: That is precisely our fear as well. That is what we are submitting to you.

[English]

The Chair: Going back over some of the same ground that has already been raised, I want to clarify some things. This goes to your first question, where I understand you to be saying that since CyberTip now does a good job with the information it receives, why bring in ISPs? Yet, as Senator Runciman noted, a lot of ISPs do not report, unfortunately, and do not participate in the voluntary efforts to track down these terrible people.

On ne dit pas nécessairement que le délai de 21 jours est trop long, mais on aimerait que cette préservation soit soumise à un mécanisme d'imputabilité comme, par exemple, une autorisation judiciaire.

Le sénateur Joyal : Vous suggérez une étape intermédiaire entre ce que nous avons actuellement dans le projet de loi et ce que vous proposez, que lorsqu'un fournisseur de services est notifié par une personne que son site sert à diffuser de la pornographie juvénile, le fournisseur se présente immédiatement devant un tribunal pour obtenir une ordonnance de conservation.

Mme Bernier : Ce n'est pas le fournisseur qui le ferait, mais il pourrait immédiatement contacter la police, laquelle pourrait intervenir et obtenir un ordre de préservation. Si c'était mieux encadré, on croit, on l'espère, et c'est sujet à considération et délibération avec d'autres témoins experts, que cela élaguerait le processus de telle façon qu'on ne recueillerait que l'information pertinente et qu'on ne viserait que les coupables. Alors on outillerait mieux les agences de sécurité pour intervenir.

Le sénateur Joyal : Vous voudriez voir un processus additionnel contenu dans le projet de loi?

Mme Bernier : Par exemple, dès que le FSI constate que son site a été utilisé pour la pornographie juvénile, qu'il le rapporte immédiatement aux agences de sécurité qui obtiendront un ordre de préservation et utiliseront l'information pour passer à l'action.

Le sénateur Joyal : Vous savez que certains cas peuvent être très évidents en regard de la pornographie infantile mais que certains autres peuvent être plus douteux. On risque de se retrouver dans la situation que nous dénonçons tantôt où, pour éviter de se retrouver en violation de la loi, on va tout rapporter pratiquement. C'est là que le projet de loi contient une difficulté additionnelle qui ne facilitera pas la lutte à la pornographie juvénile. On va se donner la bonne intention, mais il y a des mécanismes dans le projet de loi qui manquent pour rendre ce projet de loi efficace. D'autres témoins l'ont suggéré avant vous, et je crois que c'est un élément extrêmement important qu'on devrait retenir dans nos discussions sur ce projet de loi.

Mme Bernier : C'est exactement notre crainte aussi. C'est ce qu'on vous soumet.

[Traduction]

La présidente : J'aimerais revenir sur certains points qui ont déjà été soulevés pour préciser certains aspects. Cela concerne votre première question, dans laquelle vous demandiez, si j'ai bien compris, qu'étant donné que Cyberaide fait déjà du bon travail avec les renseignements que cet organisme reçoit, pourquoi faire intervenir les FSI? Et pourtant, comme le sénateur Runciman l'a noté, il y a beaucoup de FSI qui ne rapportent pas ce genre de chose, malheureusement, et qui ne participent pas aux efforts volontaires déployés pour retracer ces gens terribles.

What do we do? If I, as a citizen, stumbled upon a site like this, my instant reaction would be to call either the police or my ISP. Cybertip would not be top of mind. If I called Cybertip, I am sure they would do a wonderful job. If I called the police, I am sure they would do a wonderful job. However, if I called my ISP and it had no obligation to do anything with the information that I had provided, how else, other than a mechanism like this, would you see us handling that, as a society?

Ms. Bernier: You are speaking about the first part of section 2, the first obligation, which is the obligation to notify from the ISP. Clearly, we would want an ISP that comes across child pornography to immediately inform the police. There is no question about that.

The Chair: My question is this: Are you saying that the legal obligation to report is acceptable or not?

Ms. Bernier: We are concerned that they are put almost in an active role where they almost have to monitor. We wonder whether they are all well placed to do that. We trust some of them; they have lawyers and are well equipped to do so. However, we are afraid that too many cannot bear the responsibility that is given to them by the legislation.

The Chair: This may be a conundrum that will require all kinds of intervention to solve.

[Translation]

Senator Boisvenu: The more I listen to Ms. Bernier, the more confused I become about the position she seems to be presenting to us. First, her brief raises more questions than it answers about this bill. I would ask a direct question: is your agency in favour of this bill or not?

Ms. Bernier: Yes, absolutely.

[English]

Senator Runciman: Senator Joyal touched on something from a different perspective — the 21 days that the witness has expressed concern about — in thinking it could be compressed. There could be clearly, I would suspect, an investigative component before there is an application for a judicial order or a search warrant. The 21 days was arrived at after extensive consultation.

We heard a police witness last week who suggested that he would not mind seeing it as 31 days, but this is a compromise. I think most police agencies feel that this gives them sufficient time to carry out a necessary investigation.

The Chair: We will hear from police witnesses today.

Que pouvons-nous faire? Si moi, en tant que citoyenne, je découvre par hasard un site de ce genre, ma première réaction sera d'appeler la police ou mon FSI. Cyberaide n'est pas le nom qui me viendrait immédiatement. Si j'appelais Cyberaide, je suis sûre qu'il ferait de l'excellent travail. Si j'appelle la police, je suis sûre qu'elle fera de l'excellent travail. Cependant, si j'appelle mon FSI et qu'il n'est pas tenu de faire quoi que ce soit avec les renseignements que je lui fournis, comment notre société pourrait-elle régler ce genre de situation, s'il n'existe pas de mécanisme comme celui-ci?

Mme Bernier : Vous parlez de la première partie de l'article 2, la première obligation, qui oblige le FSI à communiquer l'adresse d'un site douteux. Il est évident que nous souhaitons que le FSI qui découvre de la pornographie juvénile en informe immédiatement la police. Cela est bien évident.

La présidente : Ma question est la suivante : trouvez-vous acceptable ou non que la loi impose l'obligation de signaler ce genre de chose?

Mme Bernier : Nous pensons que nous demandons aux FSI de jouer un rôle actif et de les obliger pratiquement à surveiller ce qui se passe. Nous nous demandons s'ils sont tous vraiment en mesure de le faire. Nous avons confiance dans un certain nombre d'entre eux; ils ont des avocats et sont bien équipés pour le faire. Nous craignons toutefois qu'il y en ait beaucoup qui ne soient pas en mesure d'assumer la responsabilité que leur impose le projet de loi.

La présidente : C'est peut-être une difficulté que l'on ne pourra résoudre qu'avec l'aide de tous les intéressés.

[Français]

Le sénateur Boisvenu : Plus j'écoute Mme Bernier, plus je suis confus dans la position qu'elle semble nous livrer. D'abord, son mémoire pose plus de questions qu'il ne statue sur ce projet de loi. Je poserais une question directe : est-ce que votre organisme est en faveur oui ou non de ce projet de loi?

Mme Bernier : Oui, absolument.

[Traduction]

Le sénateur Runciman : Le sénateur Joyal a abordé une question d'un point de vue différent — la période de 21 jours qui préoccupe le témoin — parce qu'il pensait qu'elle pouvait être réduite. Il pourrait fort bien y avoir, à mon avis, un élément d'enquête avant que la police ne présente une demande d'ordonnance ou de mandat de perquisition. La période de 21 jours a été choisie après des consultations approfondies.

Un policier qui a témoigné la semaine dernière a déclaré qu'il ne serait pas contre la prolongation de cette période, jusqu'à 31 jours, mais que c'était là un compromis. Je pense que la plupart des services de police estiment qu'ils disposent ainsi de suffisamment de temps pour effectuer l'enquête nécessaire.

La présidente : Nous allons entendre des témoins de la police aujourd'hui.

Senator Runciman: I have a question of the witness about page 4 where it says, “Consider, for instance, the potential for heightened citizen monitoring.” I do not see any requirement for citizen monitoring in this proposed legislation. Certainly, I do not interpret it that way. By asking ISPs to intrude on the private communications of Canadians would be opening the door to widespread surveillance of law-abiding citizens. That strikes me as more than a bit alarmist. How do you reach that kind of conclusion?

Ms. Bernier: I would not put it as a conclusion, but rather as a warning that any legislation that creates a framework of monitoring should be looked at —

Senator Runciman: This is not a framework for monitoring. I do not see it that way.

The Chair: Let the witness answer.

Ms. Bernier: It deputizes the ISPs to help law enforcement authorities to counter child pornography, and we are totally in favour of that. Definitely, we want to see legislation that will enhance the fight against child pornography.

We would like to put to you that you consider ensuring that this proposed legislation could not possibly open the door to surveillance of innocent law-abiding citizens, by perhaps being too broad in its wording. That is more a warning that we should not see this, as opening the door to surveillance in general.

The Chair: If I may come back to my first question, if this bill becomes law, you will have the authority to do surveillance, will you not?

Ms. Bernier: Indeed, if we received a complaint that there was an abuse by an ISP, it would be considered a violation of PIPEDA, Personal Information Protection and Electronic Documents Act, and we could investigate.

The Chair: I am sorry, Senator Runciman, but we are out of time with these witnesses, who were important to our work. We are most grateful to you for being here, Ms. Bernier and Ms. Zubrzycka. Thank you very much indeed.

We are pleased to welcome our next panel of witnesses. First, from the Canadian Centre for Child Protection is Lianna McDonald, Executive Director. Signy Arnason is Director of CyberTip. From the Ontario Provincial Police, we have Inspector Scott Naylor, Child Sexual Exploitation Section. From the Canadian Association of Chiefs of Police, we welcome Vincent Westwick, General Counsel.

Thank you all very much for being here. If you felt it was slightly short notice for us to get you here, that is the nature of the parliamentary timetable and we apologize.

Le sénateur Runciman : J’ai une question à poser au témoin au sujet de la page 4 où l’on peut lire : « Prenons, par exemple, le potentiel d’intensification des mesures de surveillance des citoyens ». Je ne vois pas que le projet de loi exige des citoyens qu’ils fassent de la surveillance. En tout cas, je ne l’interprète pas de cette façon. En demandant aux FSI de s’immiscer dans les communications privées des Canadiens, ouvrons-nous la porte à une surveillance généralisée des citoyens respectueux des lois? Cette affirmation me paraît un peu alarmiste. Comment en arrivez-vous à ce genre de conclusion?

Mme Bernier : Je ne parlerais pas de conclusion, mais plutôt d’avertissement parce que tout projet de loi qui met en place un cadre de surveillance doit être examiné...

Le sénateur Runciman : Ce n’est pas un cadre de surveillance. Je ne le vois pas de cette façon.

La présidente : Laissez le témoin répondre.

Mme Bernier : Le projet de loi demande aux FSI d’aider les autorités d’application de la loi à lutter contre la pornographie juvénile, et nous sommes totalement en faveur de cette mesure. Nous voulons bien évidemment que le projet de loi renforce la lutte contre la pornographie juvénile.

Nous aimerions vous signaler que vous devriez faire en sorte que le projet de loi ne puisse ouvrir la porte à la surveillance de citoyens innocents et respectueux des lois en choisissant une formulation qui serait trop large. C’est plus un avertissement qui nous invite à éviter ce genre de chose qu’une affirmation, à savoir que nous ouvrons la porte à la surveillance en général.

La présidente : J’aimerais revenir à ma première question, et si ce projet de loi est adopté, vous aurez le pouvoir de faire de la surveillance, n’est-ce pas?

Mme Bernier : En fait, si nous recevons une plainte indiquant qu’un FSI a abusé de sa position, cela serait considéré comme une violation de la LPRPDE, la Loi sur la protection des renseignements personnels et les documents électroniques, et nous pourrions faire enquête.

La présidente : Je suis désolée, sénateur Runciman, mais nous avons épuisé le temps prévu pour ces témoins. Leurs témoignages étaient importants pour nos travaux. Nous vous sommes très reconnaissants d’être venues, mesdames Bernier et Zubrzycka. Je vous remercie.

Nous avons le plaisir d’accueillir notre prochain groupe de témoins. Nous avons, premièrement, Lianna McDonald, directrice générale du Centre canadien de protection de l’enfance. Signy Arnason est la directrice de Cyberaide. Nous allons accueillir l’inspecteur Scott Naylor, de l’unité de la pornographie juvénile de la Police provinciale de l’Ontario. Nous allons accueillir Vincent Westwick, avocat général de l’Association canadienne des chefs de police.

Merci à tous d’être venus. Si vous pensez que vous n’avez pas eu beaucoup de temps pour vous préparer, c’est à cause de notre calendrier parlementaire et nous en sommes désolés.

Ms. McDonald, I believe you will give the opening statement. You will be followed by Inspector Naylor and then Mr. Westwick. After, we shall put questions to the lot of you.

Lianna McDonald, Executive Director, Canadian Centre for Child Protection: Thank you, Madam Chair and distinguished members of the committee. Thank you for the opportunity to provide a presentation on Bill C-22 and the larger issue of child sexual abuse on the Internet.

The Canadian Centre for Child Protection is a charitable organization dedicated to the personal safety of all children. We will offer testimony today supporting this new legislation based on our agency's role in operating Cybertip.ca, Canada's tip line to report the online sexual exploitation of children.

Cybertip was established in 2002 in partnership with the Government of Canada, various provincial governments, a national law enforcement advisory committee, a federal task force and a steering committee. Our analysts are special constables who review, confirm and triage reports to the appropriate law enforcement jurisdiction. This function permits the verification that material is potentially illegal and identifies the appropriate law enforcement jurisdiction. Specifically, the tip line accepts reports relating to child pornography, luring, child sex tourism, children exploited through prostitution, and child trafficking.

Since launching nationally, the tip line has received nearly 52,000 reports from the public regarding the online sexual exploitation of children, resulting in law enforcement executing nearly 70 arrests and with the effect of numerous children being removed from abusive environments.

Over the last 10 years of operating Cybertip, we have been better able to understand the online nature of child abuse content, and we have published research in this area. *Child Sexual Abuse Images: An analysis of websites by Cybertip.ca* reviewed approximately 15,000 child abuse websites and provided valuable information on sites that host illegal material, including the severity of abuse depicted in the images, host country locations, and other notable features on these sites. Of the webpages analyzed, 77.6 per cent had at least one child abuse image of a child less than eight years of age, with many showing infants and toddlers being sexually assaulted. At the time of analysis, nearly 60 countries were hosting this type of material and underscoring the global nature of this problem.

Madame McDonald, je crois que vous allez nous présenter un exposé d'ouverture. Vous serez suivie de l'inspecteur Naylor et ensuite, de M. Westwick. Après cela, nous vous poserons des questions.

Lianna McDonald, directrice générale, Centre canadien de protection de l'enfance : Merci, madame la présidente et distingués membres du comité. Merci de me donner la possibilité de vous présenter un exposé sur le projet de loi C-22 et sur la question plus large de l'exploitation sexuelle des enfants sur Internet.

Le Centre canadien de protection de l'enfance est un organisme de charité qui se consacre à la sécurité personnelle de tous les enfants. Nous allons offrir aujourd'hui un témoignage dans lequel nous appuyons ce nouveau projet de loi, étant donné que le rôle de notre agence est de faire fonctionner Cyberaide.ca, la ligne d'assistance canadienne où l'on peut dénoncer en direct les cas d'exploitation sexuelle des enfants.

Cyberaide a été créé en 2002 en partenariat avec le gouvernement du Canada, divers gouvernements provinciaux, un comité consultatif national d'application de la loi, ainsi qu'un groupe de travail et un comité de direction. Comme d'autres lignes internationales d'assistance, Cyberaide.ca peut compter sur des agents de police spéciaux agissant à titre d'analystes qui examinent, confirment et trient les signalements pour les envoyer aux organismes d'application de la loi compétents. Ces fonctions permettent de vérifier le matériel potentiellement illégal et de déterminer l'autorité compétente. Plus précisément, la ligne d'assistance accepte les signalements concernant la pornographie juvénile, le lurre d'enfants, le tourisme pédophile ainsi que l'exploitation d'enfants par le biais de la prostitution et le trafic d'enfants.

Depuis son lancement à l'échelle nationale, le service a reçu près de 52 000 signalements du public concernant l'exploitation sexuelle des enfants en ligne, ce qui a mené à l'arrestation de 70 personnes par les forces de l'ordre et a permis de retirer de nombreux enfants de milieux caractérisés par la violence.

Au cours des 10 dernières années de fonctionnement de Cyberaide, nous avons réussi à mieux comprendre la nature en direct du contenu constituant de l'exploitation des enfants, et nous avons publié de la recherche dans ce domaine. Notre étude intitulée *Les images d'abus pédosexuel : Analyse des sites Internet par Cyberaide.ca* recense environ 15 000 sites web de maltraitance d'enfant et fournit des renseignements utiles sur les sites qui hébergent du matériel illégal, notamment sur la gravité des abus montrés par les images, l'emplacement des pays hôtes et d'autres aspects notables de ces sites. 77,6 p. 100 des pages web analysées contenaient au moins une image d'un enfant de moins de huit ans qui était maltraité, tandis que de nombreuses autres pages montraient des enfants et des bébés en train d'être agressés sexuellement. Au moment de l'analyse, près de 60 pays hébergeaient ce genre de matériel faisant ainsi ressortir la nature mondiale du problème.

As a result, Cybertip has been working in partnership with industry, law enforcement, governments and international hotlines to reduce and disrupt the availability of child abuse websites. Recognizing the global impact of online child abuse, our agency has engaged the Internet community and wider online industry that shares our common interest in creating a safe and responsible Internet.

The Canadian Coalition Against Internet Child Exploitation, CCAICE, is a voluntary partnership between Cybertip, law enforcement and the private sector to address the sexual exploitation of children. We have realized a number of important successes. One such example includes Cleanfeed Canada, a solution to block access to foreign-based websites hosting child pornography. All of the major ISPs participate in this program and, to date, approximately 14,000 URLs have been put on this list, as well as 122,000 child abuse images, blocking this harmful material from the view of most Canadians.

We support Bill S-22 because it rightly addresses the challenges regarding Internet-related child abuse and exploitation.

There are two co-existing realities surrounding how the web facilitates child abuse and exploitation. The first problem is the publicly available child abuse material and content, usually in the form of websites. The second is how offenders use Internet services to facilitate the abuse of children. This would include the online storage of child pornography, sharing illegal material, and promoting such activities among individuals and online communities.

As the front door to the Canadian public for reporting, we have learned a few things. Up to 81 per cent of all reports submitted pertain to website content, of which the majority is hosted outside of Canada's borders. Roughly 19 per cent of potentially illegal websites are forwarded to Canadian law enforcement agencies. The triaging role of the tip line allows Canadian law enforcement to focus their limited resources on investigations within their jurisdiction.

The results and impact of mandatory reporting are evident in other jurisdictions. Cybertip is the designated reporting agency under Manitoba's mandatory reporting of child pornography legislation. Public reporting increased by 126 per cent in the first year that the legislation was enacted when compared to the previous year. The tip line triaged reports, which resulted in 17 reports containing information on an identified child victim and/or suspect in Manitoba being forwarded to a child welfare agency.

C'est pourquoi Cyberaide travaille en partenariat avec l'industrie, les organismes d'application de la loi, les gouvernements et les lignes d'assistance internationales dans le but de rendre plus difficile l'accès aux sites web qui montrent des enfants agressés et pour en perturber le fonctionnement. Notre agence sait que l'agression des enfants en direct a des répercussions mondiales et elle a recherché la collaboration de la communauté Internet et de l'industrie des services en ligne qui partagent notre volonté de créer un Internet sûr et responsable.

La Coalition canadienne contre l'exploitation des enfants sur Internet, également appelée CCCEEI, est un partenariat volontaire qui regroupe Cyberaide, les forces de l'ordre et le secteur privé afin de lutter contre l'exploitation sexuelle des enfants. Nous avons remporté quelques victoires importantes. Cleanfeed Canada, une solution visant à bloquer l'accès aux sites web basés à l'étranger qui hébergent de la pornographie juvénile, en est un exemple. Tous les principaux fournisseurs de services Internet participent à ce programme et jusqu'à maintenant, plus de 14 000 adresses URL ont été placées sur cette liste, ainsi que 122 000 images représentant des enfants agressés, ce qui a permis de bloquer l'accès à ce matériel préjudiciable pour la majorité des Canadiens.

Nous sommes en faveur du projet de loi C-22 parce qu'il répond de façon appropriée aux défis que posent l'exploitation et l'agression des enfants par le biais d'Internet.

Le web facilite la direction et l'exploitation des enfants de deux façons qui se renforcent l'une l'autre. Le premier problème est le matériel et le contenu représentant des enfants agressés, qui sont mis à la disposition du public, habituellement sous la forme de sites web. Le deuxième vient des façons dont les délinquants utilisent les services Internet pour faciliter l'agression des enfants. Cela comprend notamment le stockage en ligne de pornographie juvénile, le partage de matériel illégal et la promotion de ces activités entre individus et collectivités en ligne.

En tant qu'organisme de première ligne pour les signalements transmis par les Canadiens, nous avons appris un certain nombre de choses. Près de 81 p. 100 de tous les signalements reçus concernent le contenu de sites web, dont la plupart se trouvent à l'étranger. Près de 19 p. 100 des sites web apparemment illégaux sont signalés aux organismes canadiens d'application de la loi. Le tri qu'effectue la ligne d'assistance permet aux organismes canadiens d'application de la loi de concentrer leurs ressources limitées sur les enquêtes relevant de leur compétence.

Les résultats et les impacts de la déclaration obligatoire sont manifestes dans d'autres provinces. Cyberaide est l'organisme de déclaration désigné en vertu de la Loi sur la déclaration obligatoire de la pornographie juvénile du Manitoba. Les signalements par le public ont augmenté de 126 p. 100 la première année de mise en œuvre de cette loi par rapport à l'année précédente. La ligne d'assistance a traité les signalements reçus, dont 17 ont fourni des informations liées à une jeune victime ou à un suspect et ont été transmis à une agence de protection de l'enfance du Manitoba.

The public nature of the Internet, combined with the viral nature of child pornography, offers the opportunity for the public and Internet service providers to report and assist in the detection of this material. Bill S-22 will not only assist in reducing child pornography on the Internet, but will more importantly potentially identify victims and their abusers. Mandatory reporting legislation removes the professional and personal dilemma of reporting. It clarifies and reinforces what the major Internet access providers are already doing and offers protection for appropriate action.

Legislation also becomes a deterrent and sends the message that Canada will not become a haven for child abuse images and websites. Those profiting off the abuse of children often deliberately move content to avoid detection. Countries with strong legislation create a disincentive for those involved in providing access to the illegal material. Enacting mandatory reporting legislation demonstrates a cognizance that society as a whole has a moral obligation to protect its most vulnerable citizens. Placing the legal onus on those providing an Internet service should they become aware of illegal material would strengthen Canada's role in tackling this global problem.

In conclusion, good legislation, adequate resources, global cooperation, technical solutions and public education are key components to getting ahead of this problem. Canada's decision to take this additional step sends a clear and strong message to its citizens and other countries that children are a national priority.

I want to just mention a few notes that my colleague would have mentioned quickly in terms of some of the statistics. There were a lot of questions surrounding volume. Again, the reporting triaging function is key. When we look at the 52,000 reports, the majority of these dealing with websites, 91 per cent of those reports were classified as child pornography and were predominantly entered through our online report form. Of the total number of those reports, 81 per cent pertain to website content.

In terms of our overall triaging rates, 46 per cent of reports that come in go to law enforcement and/or our international hotline partners. This means that law enforcement is dealing with roughly 50 per cent of the reports that we receive. Of the 40,000 reports processed since April 2008, 4,200 were sent to Canadian law enforcement agencies.

Finally, as a tip line operating, we receive these reports 24 hours a day, 7 days a week and we have a 48-hour turnaround time. These are basic statistics for Cybertip.ca and some information as to why we support Bill C-22. Thank you for the opportunity to present.

La nature publique d'Internet, combinée à l'effet contagieux de la pornographie juvénile, donne au public et aux fournisseurs de services Internet la possibilité de signaler ce matériel et d'aider à sa détection. Le projet de loi C-22 aidera non seulement à réduire la pornographie juvénile affichée sur Internet, mais aidera surtout à identifier les victimes et leurs agresseurs. Les dispositions imposant l'obligation de signaler ces sites feront disparaître le dilemme personnel et professionnel que posent parfois les signalements. Elles vont préciser et renforcer ce que les principaux fournisseurs de services Internet font déjà et les protégeront lorsqu'ils interviendront.

Ces mesures législatives ont également un effet dissuasif et font clairement savoir que le Canada se refuse d'être un refuge pour les images et les sites web consacrés à l'exploitation des enfants. Ceux qui profitent de l'exploitation des enfants déplacent bien souvent, délibérément, ce contenu pour éviter d'être repérés. Les pays qui ont adopté des lois rigoureuses incitent les personnes susceptibles de fournir un accès à ce matériel illégal à s'en abstenir. L'adoption de dispositions exigeant le signalement reflète le principe que la société tout entière a l'obligation morale de protéger les citoyens les plus vulnérables. Obliger légalement les personnes qui fournissent des services Internet à signaler le matériel illégal dont elles prennent connaissance renforcera le rôle que joue le Canada dans la lutte contre ce problème mondial.

En conclusion, de bonnes mesures législatives, des ressources adéquates, une collaboration internationale, des solutions techniques et la sensibilisation du public sont les composants essentiels d'une solution qui permettra de remédier à ce problème. La décision qu'a prise le Canada d'adopter ces mesures supplémentaires fait clairement savoir à ses citoyens et aux autres pays que les enfants sont une priorité nationale.

Je vais mentionner quelques données que mon collègue vous aurait fournies rapidement sur le plan des statistiques. On a posé beaucoup de questions sur le nombre des signalements. Encore une fois, le tri des signalements est un élément clé. Dans le cas de ces 52 000 signalements, dont la majorité concernait des sites web, 91 p. 100 d'entre eux ont été classés comme constituant de la pornographie juvénile et ont été reçus pour la plupart par le formulaire de signalement en direct. Quarante-vingt-un pour cent du nombre total de ces signalements concernaient un contenu affiché sur le site web.

Pour ce qui est de nos taux généraux de tri, 46 p. 100 des signalements reçus sont transmis à nos partenaires d'application de la loi ou aux lignes d'assistance internationales. Cela veut dire que les services d'application de la loi examinent près de 50 p. 100 des signalements que nous recevons. Sur les 40 000 signalements traités depuis avril 2008, 4 200 ont été transmis aux agences canadiennes d'application de la loi.

Enfin, en tant que ligne d'assistance, nous recevons ces signalements 24 heures par jour et sept jours par semaine et nous les traitons dans les 48 heures. Ce sont là les statistiques de base de Cyberaide.ca qui expliquent en partie pourquoi nous sommes en faveur du projet de loi C-22. Merci de m'avoir donné la possibilité de vous présenter notre point de vue.

The Chair: Thank you very much. I apologize for the fact that you are required to compress so much knowledge and experience into such a short time, but from our point of view, everything you give us is precious, even if it is compressed.

Inspector Scott Naylor, Manager, Child Sexual Exploitation Section, Ontario Provincial Police: Good evening. Thank you for the opportunity to offer some insight from a law enforcement perspective and provide comment regarding Bill C-22.

I am the manager of the OPP, Ontario Provincial Police, Child Sexual Exploitation Section. Our most fundamental responsibility as a society is to protect our children from those who would do them harm.

The Internet provides many excellent learning opportunities for children. It also opens another door for predators that would exploit and abuse children. A recent study shows that 94 per cent of Canadian children have access to the Internet and 40 per cent have their own Internet high-speed access.

Members of the OPP Child Sexual Exploitation Section and the OPP-led Ontario provincial strategy to protect children from sexual abuse and exploitation on the Internet have laid numerous charges through coordinated child sexual abuse (pornography) investigations.

From January 1, 2010, to February 16, 2011, the provincial strategy completed 2,578 investigations and laid 829 charges against 218 people. Eighty-four child victims were identified during that period. Over the same 11-month period, the OPP Child Sexual Exploitation Section investigated an additional 359 cases and laid 252 charges against 50 people. Thirty-seven additional child victims were identified.

This is a very big problem that cannot be overlooked. Child sexual exploitation in the Internet is child abuse, plain and simple. Every depiction of a child being abused through videos and photos, or downloaded and shared through peer-to-peer networks and ISP servers, represents a revictimization of that child.

The Ontario police services associated with the provincial strategy will stop at nothing to hunt down child predators and eliminate the threat they pose to our children and our communities.

It takes an enormous amount of resources and coordination for any police service to carry out Internet luring and child sexual abuse investigations. In recent weeks, we and our partners have made a large number of arrests in various parts of Ontario. These investigations have ties to other parts of Canada and across North America. The range in ages of those charged runs a wide

La présidente : Merci. Je vous prie de m'excuser de vous avoir demandé de condenser toutes ces connaissances et toute cette expérience dans un temps aussi court, mais de notre point de vue, tout ce que vous nous communiquez est précieux, même si c'est très résumé.

Inspecteur Scott Naylor, Unité de la pornographie juvénile, Police provinciale de l'Ontario : Bonsoir. Merci de me donner la possibilité de vous fournir le point de vue de l'application de la loi et de vous présenter des commentaires au sujet du projet de loi C-22.

Je suis le responsable de l'Unité de la pornographie juvénile de la Police provinciale de l'Ontario, la PPO. La principale responsabilité de notre société est de protéger nos enfants contre ceux qui voudraient leur nuire.

Internet offre d'excellentes possibilités d'apprentissage aux enfants. Il ouvre également la porte aux prédateurs qui veulent exploiter et maltraiter les enfants. D'après une étude récente, 94 p. 100 des enfants canadiens ont accès à Internet et 40 p. 100 d'entre eux ont leur propre accès à Internet à haute vitesse.

Les membres de l'unité de la pornographie juvénile de la PPO et les partenaires de la stratégie provinciale de l'Ontario que dirige la PPO en vue de protéger les enfants contre l'exploitation et l'agression sexuelles sur Internet ont déposé de nombreuses accusations grâce à des enquêtes coordonnées sur les cas d'exploitation sexuelle d'enfants (pornographie).

Du 1^{er} janvier 2010 au 16 février 2011, les partenaires de la stratégie provinciale ont achevé 2 578 enquêtes et porté 829 accusations contre 218 personnes. Quarante-vingt-quatre enfants victimes ont été identifiés au cours de cette période. Pendant la même période de 11 mois, l'unité de la pornographie juvénile de la PPO a fait enquête sur 359 autres affaires et porté 252 accusations contre 50 personnes. Trente-sept enfants victimes supplémentaires ont été identifiés.

C'est là un problème très grave qu'on ne peut mettre de côté. L'exploitation sexuelle d'enfants sur Internet est de l'agression contre les enfants, cela est clair. Chaque fois que l'on montre un enfant en train d'être agressé dans des vidéos et des photos, ou sur des fichiers téléchargés et partagés sur des réseaux pair-à-pair et des serveurs FSI, on montre une nouvelle fois cet enfant en train d'être victimisé.

Les services de police de l'Ontario associés à ses partenaires de la stratégie provinciale ne ménagent aucun effort pour pourchasser les prédateurs des enfants et supprimer la menace qu'ils représentent pour les enfants et nos collectivités.

Il faut énormément de ressources et de coordination pour qu'un service de police puisse effectuer des enquêtes sur l'exploitation sexuelle d'enfants et le leurre d'enfants sur Internet. Ces dernières semaines, nous et nos partenaires avons procédé à un grand nombre d'arrestations dans diverses régions de l'Ontario. Ces enquêtes ont eu des ramifications dans d'autres

and troubling gamut from mid-teens to senior citizens. In many of these cases, these are return customers, those who have previously offended.

We, as law enforcement, are also keenly aware that we cannot succeed in protecting children in isolation. Unfortunately, most parents and guardians are lagging far behind their children in their understanding of web technology and the ever-burgeoning world of social media. Parents and guardians need to educate themselves to keep children safe and keep Internet predators out of our real and virtual communities.

The OPP and its provincial strategy partners have been working diligently with others to create public education and awareness opportunities in communities, online and on television for kids, parents and guardians, but there are also ways that government can assist in keeping our children and communities safe — through effective legislative tools that will assist with police investigations.

It is my opinion, and the opinion of the Ontario Provincial Police, that Bill C-22 proposes another tool so that we may help advance our investigations and enhance public safety. This bill will effectively shine a public light on those websites, files and images of child sexual exploitation that have been previously and purposely shrouded in secrecy.

Currently, Internet service providers are served with search warrants, production orders or a law enforcement request for the subscriber information relating to a particular Internet protocol or IP address. This can be time consuming and cumbersome, and, in effect, protects the identities of child predators and the materials they produce.

If passed, the legislation being introduced by the Government of Canada will further strengthen our relationships with Internet service providers, and enhance the ability to obtain vital information and launch investigations quickly, which helps ensure the safety of children.

The OPP and the provincial strategy to protect children from sexual abuse and exploitation on the Internet are working. They continue to work to make our children and our communities safer. Tremendous dedication, collaboration and hard work are required in order to coordinate these investigations. All Ontario police services take this responsibility very seriously. We coordinate our limited resources to protect children from online predators.

The OPP and the provincial strategy partners appreciate any legislative tools that can be brought to bear on those who would commit these horrific crimes against society's most precious resource — our children.

régions du Canada et dans toute l'Amérique du Nord. L'âge des personnes accusées représente une gamme très large et troublante qui va des adolescents aux personnes âgées. Bien souvent, ce sont des récidivistes, des personnes qui ont déjà commis des infractions de ce genre.

Nous, les membres des services d'application de la loi, savons trop bien que nous ne pouvons pas protéger les enfants en agissant seuls. Malheureusement, la plupart des parents et des gardiens connaissent beaucoup moins bien que les enfants la technologie web et le monde en plein développement que sont les médias sociaux. Il faut que les parents et les gardiens commencent par s'informer s'ils veulent protéger leurs enfants et exclure de nos collectivités réelles et virtuelles les prédateurs qui utilisent Internet.

La PPO et ses partenaires de la stratégie provinciale ont beaucoup travaillé avec d'autres intéressés pour offrir des services de sensibilisation et d'éducation publique dans les collectivités, en ligne et à la télévision pour les enfants, les parents et les tuteurs. Le gouvernement peut également prendre des mesures pour assurer la sécurité de nos enfants et de nos collectivités — l'adoption d'outils législatifs efficaces qui faciliteront les enquêtes policières.

Je pense, et c'est également l'opinion de la Police provinciale de l'Ontario, que le projet de loi C-22 offre un autre outil qui pourra faciliter nos enquêtes et renforcer la sécurité de la population. Ce projet de loi va jeter un éclairage public sur les sites web, les fichiers et les images d'exploitation sexuelle d'enfants qui étaient jusqu'ici délibérément clandestins.

À l'heure actuelle, les fournisseurs de services Internet se voient signifier des mandats de perquisition, des ordonnances de communication et des demandes de la part des services d'application de la loi en vue d'obtenir des renseignements sur les abonnés reliés à une adresse IP ou un protocole Internet particulier. Cela prend beaucoup de temps et c'est un processus lourd qui, en réalité, protège l'identité des prédateurs d'enfants et le matériel qu'ils produisent.

S'il est adopté, le projet de loi proposé par le gouvernement du Canada va renforcer nos relations avec les fournisseurs de services Internet, et améliorer notre capacité d'obtenir des renseignements vitaux et de lancer rapidement des enquêtes, ce qui protégera mieux les enfants.

La PPO et les membres de la stratégie provinciale visant à protéger les enfants contre l'exploitation et les abus sexuels sur Internet obtiennent des résultats. Ils continuent leur travail pour renforcer la sécurité de nos enfants et de nos collectivités. Il faut être très concentré, collaborer et travailler beaucoup pour réussir à coordonner ces enquêtes. Tous les services de police de l'Ontario prennent cette responsabilité très au sérieux. Nous coordonnons nos ressources limitées pour protéger les enfants contre les prédateurs d'Internet.

La PPO et nos partenaires de la stratégie provinciale se félicitent de voir proposer des mesures législatives qui leur donneront des outils pour lutter contre ceux qui commettent des crimes horribles contre la ressource la plus précieuse de notre société — les enfants.

Child pornography is a problem. It is in every community and continues to have a devastating effect on our children and our society.

Thank you again for taking the time to consider this important legislation, and for the opportunity to present my views and opinions from a law enforcement perspective.

Remember: Every child matters, everywhere.

The Chair: Thank you very much. Mr. Westwick.

Vincent Westwick, General Counsel, Canadian Association of Chiefs of Police: Child pornography is a special crime. Some years ago, I brought samples of child pornography to a parliamentary committee studying changes to the pornography sections of the Criminal Code. The thinking was that it was important for parliamentarians to actually see the kind of material that is being produced and distributed in Canadian communities. In spite of my full career in criminal justice, I was shocked, even stunned, by what I saw, and certainly shared the horror and outrage of parliamentarians.

It is with that sentiment in mind that I speak to you today. It is therefore very easy to stand before you, figuratively speaking, to support any legislation which addresses this most serious and heinous social problem.

I am joined today by Constable Frank Corkery, who is sitting in the back, from the Ottawa Police Service. Frank is a member of the high-tech crime Internet child exploitation unit, ICE. It is Constable Corkery's job to investigate in the area of high-tech crime and Internet crimes against children. He is available to the committee to provide that important front-line perspective. He is also part of Inspector Naylor's provincial strategy.

In the criminal sphere, Parliament passes different types of legislation. Some create new offences, some address evidentiary issues and others give direction on sentencing. Bill C-22 is different. Bill C-22 is what I call an "investigative assist". It provides a legislative assist to police in detecting and investigating crimes. This is an important type of bill. Police must be able to get child pornographers into the courtroom.

Bill C-22 also inherently recognizes that the world of child pornography has changed. For example, many years ago, when I was investigating child pornography as a police officer, I was told to watch for men wearing long raincoats, and who kept their pornography in a brown paper bag. Now, in our technological age, to speak in those terms seems laughable.

La pornographie juvénile est un problème. On la trouve dans chaque collectivité et elle continue d'avoir un effet dévastateur sur nos enfants et notre société.

Je vous remercie encore une fois de prendre le temps d'examiner cette importante mesure législative et de nous avoir donné la possibilité de présenter mes commentaires et mes opinions du point de vue de l'application de la loi.

N'oubliez pas : chaque enfant est important, où qu'il soit.

La présidente : Merci. Monsieur Westwick.

Vincent Westwick, avocat général, Association canadienne des chefs de police : La pornographie juvénile est un crime particulier. Il y a quelques années, j'ai présenté quelques exemples de pornographie juvénile à un comité parlementaire qui étudiait les changements à apporter aux dispositions du Code criminel concernant la pornographie. J'avais pensé qu'il était important que les parlementaires se rendent compte personnellement du matériel qui était produit et distribué dans les collectivités canadiennes. Malgré ma longue carrière au sein du système de justice pénale, j'ai été choqué, et même bouleversé, par ce que j'ai vu et j'ai également partagé le sentiment d'horreur et d'outrage ressenti par les parlementaires.

C'est avec ce sentiment que je vous parle aujourd'hui. Il m'est donc très facile d'être ici aujourd'hui pour appuyer une mesure législative qui porte sur un problème social particulièrement grave et choquant.

Je suis accompagné aujourd'hui par l'agent Frank Corkery, qui est assis derrière moi, un membre du Service de police d'Ottawa. Frank fait partie de l'unité de lutte contre l'exploitation des enfants sur Internet et des crimes de haute technologie. Son travail consiste à faire enquête sur les crimes commis contre les enfants sur Internet. Il est ici pour fournir au comité l'important point de vue d'un agent de première ligne. Il participe également à la stratégie provinciale de l'inspecteur Naylor.

Dans le domaine du droit pénal, le législateur adopte différents types de lois. Certaines créent de nouvelles infractions, d'autres portent sur des questions de preuve, et d'autres contiennent des directives en matière de peine. Le projet de loi C-22 est différent. Le projet de loi C-22 serait ce que j'appelle une loi d'« aide aux enquêtes ». Il fournit une assistance législative aux services de police dans le domaine de la détection et des enquêtes sur les crimes. C'est un type de projet de loi très important. Les policiers doivent pouvoir traduire devant les tribunaux les auteurs de pornographie juvénile.

Le projet de loi C-22 tient naturellement compte du fait que le monde de la pornographie juvénile a changé. Par exemple, lorsqu'il y a des années, je faisais enquête sur la pornographie juvénile en tant qu'agent de police, on m'avait dit de surveiller les hommes qui portaient de longs imperméables, et qui gardaient leur matériel pornographique dans un sac de papier brun. Aujourd'hui, à notre ère technologique, il semble ridicule de parler de cette façon.

Officers such as Constable Corkery and Inspector Naylor are now investigating sophisticated criminals with a high level of technological knowledge, and who use complex computer processes to commit their crimes. Emerging technologies are being usurped. Today's child pornographer knows how to use technology to frustrate detection and to defeat the collection of evidence that can be used in the courtroom. What has not changed is the gravity of the offence and its immeasurable impact on children.

Putting a positive duty on Internet providers to report is an important investigative assist. To the police, it is a starting point, a lead, a place to begin the investigation. Sometimes it is information that the police might not otherwise obtain. Also, knowing that an Internet service provider will be required by law to report child pornography on their system may deter a child pornographer from his actions. That, too, is a positive consequence.

I am here today representing the Ottawa Police Service, but I also serve as the co-chair of the law amendments committee of the Canadian Association of Chiefs of Police, CACP. I am therefore pleased to convey greetings and the support of both Chief Vern White of the Ottawa Police Service and Chief Bill Blair of the Toronto Police Service, who is the current president of the CACP. Bill C-22 is important legislation and should be passed.

The Chair: Thank you all very much indeed. Thank you for keeping things as tight as you have done.

Senator Wallace: Thank you for your presentations.

Ms. McDonald, I direct my first question to you. In your presentation, I was particularly drawn by your comment that, when Manitoba moved to a mandatory reporting system from a voluntary one, in the first year the reporting of pornography online increased by 126 per cent. Obviously, it would seem to show that the mandatory system produced the needed results.

Your organization receives tips from a number of sources, such as members of the public and Internet service providers. Can you tell us anything about the percentage of, or the trends in, reporting from Internet service providers? Of the total tips you receive, what percentage would come from the public versus from Internet service providers? Within the Internet service providers, what is the trend? Are they receiving more or fewer tips over the past few years?

Ms. McDonald: It is difficult for us to say specifically how many of our total number of reports pertain to Internet service providers. Currently, we do not separate that information in terms of industry reporting, so I do not have those numbers for

Les officiers de police comme l'agent Corkery et l'inspecteur Naylor font aujourd'hui enquête sur des criminels sophistiqués qui ont une grande connaissance des ressources qu'offre la technologie et qui utilisent des processus informatiques complexes pour commettre leurs crimes. Ils s'emparent des technologies émergentes. Les auteurs de pornographie juvénile d'aujourd'hui savent comment utiliser la technologie pour empêcher d'être découverts et pour bloquer la collecte de preuves utilisables devant un tribunal. Ce qui n'a pas changé, c'est la gravité de l'infraction et ses effets considérables sur les enfants.

L'imposition aux fournisseurs de services Internet de l'obligation de signaler ce genre de cas aidera beaucoup nos enquêtes. Pour la police, c'est un point de départ, une piste, un endroit où commencer une enquête. C'est parfois des renseignements que la police ne pourrait pas se procurer autrement. En outre, le fait de savoir qu'un fournisseur de service Internet est légalement tenu de signaler la pornographie juvénile présente sur son système risque de dissuader les auteurs de pornographie juvénile d'agir dans ce domaine. C'est là une autre conséquence positive.

Je représente ici aujourd'hui le Service de police d'Ottawa, mais je suis également coprésident du comité des modifications législatives de l'Association canadienne des chefs de police, ACCP. J'ai donc le plaisir de vous transmettre les salutations et l'appui du chef Vern White du Service de police d'Ottawa et du chef Bill Blair du Service de police de Toronto, qui est le président actuel de l'ACCP. Le projet de loi C-22 est une mesure législative importante qui devrait être adoptée.

La présidente : Merci. Merci d'avoir été aussi concis que vous l'avez été.

Le sénateur Wallace : Merci pour vos exposés.

Madame McDonald, je vais vous adresser ma première question. Dans votre exposé, j'ai été particulièrement frappée par votre commentaire selon lequel, lorsque le Manitoba a adopté un système de signalement obligatoire et non pas de signalement volontaire, le nombre des signalements de pornographie en ligne a augmenté de 126 p. 100 la première année. Il est évident que ce système de signalement obligatoire a donné les résultats espérés.

Les renseignements que votre organisme reçoit proviennent d'un certain nombre de sources, comme les membres du public et les fournisseurs de services Internet. Pouvez-vous nous parler du pourcentage des signalements transmis par les fournisseurs de services Internet ou des tendances dans ce domaine? Parmi tous les signalements que vous recevez, quel est le pourcentage d'entre eux qui viennent du public et ceux qui viennent des fournisseurs de services Internet? Au sein des fournisseurs de services Internet, quelle est la tendance générale? Reçoivent-ils davantage ou moins de renseignements que ces dernières années?

Mme McDonald : Il nous est difficile de préciser le nombre des signalements qui proviennent des fournisseurs de services Internet parmi tous ceux que nous recevons. À l'heure actuelle, nous ne faisons pas de distinction sur ce plan, pour ce qui est des

you. Additionally, because much of the material that companies and individuals may come across pertains to websites, often they will not provide identifying information to that end.

Signy Arnason, Director, Cybertip.ca, Canadian Centre for Child Protection: I would add that, certainly, the vast majority of what comes in either comes from the Canadian public or from other countries around the world. In particular, we work closely with other hotlines. Once they identify that the jurisdiction may pertain to Canada, the information is forwarded directly to us. We predominantly receive our information from other hotlines or members of the public. As Ms. McDonald noted, you can come in and supply us with the URL and not have to provide any other information. Therefore, we would not be able to qualify how many of the ISPs come in to report.

Senator Wallace: Regardless of where reporting is coming from, is it fair to say from your experience that moving from a voluntary reporting system to a mandatory system will enhance greatly the opportunity to detect, and then take action against perpetrators of online problems?

Ms. McDonald: Certainly, we support the legislation. I will add, as mentioned in my presentation, that while we know that the majority of the major ISPs are reporting on a voluntary basis, this proposed legislation rightly covers content hosting providers. Definitely, we know through our research that we have a problem with content being hosted in Canada. This bill will require them to take action.

Senator Wallace: Inspector Naylor, I have a quick question to you along the same line. What is your comment as one who has seen these problems and worked with them for many years on the enforcement side? What is your comment about the current voluntary reporting system or lack of system versus a mandatory system as proposed in Bill C-22? Do you see moving to mandatory reporting as a significant improvement?

Mr. Naylor: Yes. We receive a significant number of reports from Cybertip. I have to bank on some of the information that Ms. McDonald has said as well. This is a positive move forward that will increase our workload because many reports out there are going unnoticed because there is no formalized reporting legislation for the ISPs.

Senator Wallace: Presumably, the result of that will be a shutdown in greater numbers of these offensive websites that create the problems. Ultimately, that is the objective.

Mr. Naylor: Yes.

Senator Angus: I thank all of you for coming today. Inspector Naylor, could you turn to page 8 of your opening statement? I believe there is a typo, or perhaps I need a clarification. Where the third paragraph states, "It is . . . the opinion of the Ontario

signalements provenant de ce secteur; je ne peux donc pas vous fournir ces chiffres. En outre, étant donné qu'une bonne partie du matériel que les entreprises et les individus découvrent concerne des sites web, ils ne fournissent pas toujours des renseignements concernant ces aspects.

Signy Arnason, directrice, Cyberaide.ca, Centre canadien de protection de l'enfance : Je dirais que l'immense majorité des signalements viennent du public canadien ou de pays étrangers. En particulier, nous collaborons étroitement avec les autres lignes d'assistance. Dès qu'elles apprennent qu'un signalement concerne peut-être le Canada, l'information nous est directement transmise. Nous recevons l'essentiel de nos renseignements d'autres lignes d'assistance et de membres du public. Comme l'a noté Mme McDonald, vous pouvez entrer sur notre site et nous fournir une adresse URL, sans avoir à donner aucune autre information. C'est la raison pour laquelle nous ne sommes pas en mesure de vous dire combien de FSI nous transmettent des signalements.

Le sénateur Wallace : Quelle que soit l'origine du signalement, peut-on dire, d'après votre expérience, que le fait de passer d'un système de signalement volontaire à un système obligatoire va grandement renforcer la capacité de découvrir les auteurs de ces infractions commises en ligne pour ensuite prendre des mesures contre eux?

Mme McDonald : Nous sommes évidemment en faveur de ce projet de loi. J'ajouterais, comme je l'ai mentionné dans mon exposé, que, si la majorité des principaux FSI signalent volontairement ce genre de situation, le projet de loi vise avec raison les fournisseurs d'hébergement de contenu. Effectivement, nous avons appris grâce à notre recherche que du contenu de ce genre est hébergé au Canada. Ce projet de loi les obligera à réagir.

Le sénateur Wallace : Inspecteur Naylor, j'aimerais vous poser une brève question sur le même sujet. Quel commentaire aimeriez-vous faire en tant que personne qui connaît ces problèmes et qui a travaillé dans ce domaine pendant des années du côté de l'application de la loi? Que pensez-vous du système actuel de signalement volontaire ou d'absence de système par rapport au système que propose le projet de loi C-22? Pensez-vous que le signalement obligatoire constitue une amélioration importante?

M. Naylor : Oui. Nous recevons un grand nombre de signalements de Cyberaide. J'utilise également les renseignements dont Mme McDonald a parlé. C'est une mesure très positive qui va augmenter notre charge de travail parce qu'il n'existait pas auparavant de loi obligeant officiellement les FSI à fournir ces signalements, qui n'étaient donc pas transmis.

Le sénateur Wallace : Il est possible d'espérer qu'avec ce projet de loi, nous réussirons à fermer davantage de sites web illégaux qui sont à l'origine de ces problèmes. C'est l'objectif ultime.

M. Naylor : Oui.

Le sénateur Angus : Je vous remercie tous d'être venus. Inspecteur Naylor, ne pourriez-vous examiner la page 8 de votre déclaration d'ouverture? Je crois qu'il y a une erreur de frappe, ou j'aurais peut-être besoin d'une précision. On peut lire

Provincial Police that Bill C-22 proposes another tool that we may help. . .” Are you saying that it may help? What is meant by that line?

Mr. Naylor: I am sorry; it will help, absolutely.

Senator Angus: There is no issue.

Mr. Naylor: There is absolutely no doubt that there is a typo.

Senator Angus: You were so positive about the bill I thought it must be a typo. You talked about the provincial strategy partners. Are they different police forces?

Mr. Naylor: Yes.

Senator Angus: Are they only in Ontario?

Mr. Naylor: I am here to represent Ontario. The provincial strategy is 18 police services with 53 members from municipal agencies as well as the OPP. In 2006, the Government of Ontario pooled resources, as opposed to every municipal police organization doing things a separate way, to put together a joint force. It is working very effectively to standardize training, methodology and operating procedures across Ontario.

Senator Angus: It is not a national organization.

Mr. Naylor: It is not a national organization but, currently, it is being modeled across the country. It is not formalized yet but people are aspiring to follow it.

Senator Angus: Ms. McDonald, I believe that Mr. Westwick referred to your organization as one of the partners. I would like to know a little more about your charitable organization. I am impressed by all this material you have brought, including the list of your sponsors and supporters. Is your organization in Ontario only?

Ms. McDonald: No. We are a national organization. Our organization was established specifically to manage the online reporting of child pornography. We were set up in 2002 with a number of stakeholders who contributed to the establishment of Cybertip.ca. The mandate is two pronged: First, we accept reports from the Canadian public regarding the online sexual exploitation of children; and second, we carry out mass public education campaigns on this issue.

Senator Angus: It seems like such a tremendous organization. Although the answers to my questions might be in all these papers, I will ask: How many employees do you have? Are they employees or are they volunteers?

Ms. McDonald: They are all employees.

au troisième paragraphe : « La Police provinciale de l’Ontario estime que le projet de loi C-22 propose un autre outil que nous pourrions peut-être aider [...] ». Dites-vous qu’il pourrait aider? Que voulez-vous dire?

M. Naylor : Excusez-moi; il va aider, absolument.

Le sénateur Angus : Cela est certain.

M. Naylor : Il est absolument certain qu’il y a une erreur de frappe.

Le sénateur Angus : Vous étiez tellement positif au sujet du projet de loi que j’ai pensé que ce devait être une erreur. Vous avez parlé des partenaires de la stratégie provinciale. Sont-ils d’autres services de police?

M. Naylor : Oui.

Le sénateur Angus : Uniquement de l’Ontario?

M. Naylor : Je représente ici l’Ontario. La stratégie provinciale regroupe 18 services de police et 53 membres des agences municipales ainsi que la PPO. En 2006, le gouvernement de l’Ontario a regroupé les ressources, pour que chaque service de police municipal ne fasse pas les choses de son côté et de façon à mettre sur pied un groupe mixte. Il a beaucoup fait pour normaliser la formation, la méthodologie et la procédure opérationnelle dans la province de l’Ontario.

Le sénateur Angus : Ce n’est pas une organisation nationale.

M. Naylor : Ce n’est pas une organisation nationale, mais à l’heure actuelle, elle sert de modèle dans différentes régions du pays. Cette organisation n’est pas encore officialisée, mais les gens veulent s’en inspirer.

Le sénateur Angus : Madame McDonald, je pense que M. Westwick a parlé de votre organisation comme un groupe de partenaires. J’aimerais en savoir davantage au sujet de votre organisme de charité. Je suis impressionné par tous les documents que vous avez apportés, y compris la liste de vos commanditaires et des groupes qui vous accordent un appui financier. Votre organisation exerce-t-elle ses activités uniquement en Ontario?

Mme McDonald : Non. Nous sommes une organisation nationale. Notre organisation a été créée expressément pour s’occuper du signalement en ligne de la pornographie juvénile. Nous avons été créée en 2002 par un certain nombre d’intéressés qui ont participé à la mise sur pied de Cyberaide.ca. Notre mission est double : premièrement, nous acceptons les signalements émanant du public canadien au sujet de l’exploitation sexuelle en direct des enfants, et deuxièmement, nous lançons des campagnes d’éducation du public sur ces questions.

Le sénateur Angus : Cela semble être une excellente organisation. Il est possible que les réponses à mes questions se trouvent toutes dans ces documents, mais je vais vous demander : combien avez-vous d’employés? Sont-ce des employés ou des bénévoles?

Mme McDonald : Ce sont tous des employés.

Ms. Arnason: Working on the tip line, we have seven analysts and four technical staff as well as me as the director. The entire organization has 40 employees. In terms of the work on the tip line, we do not have volunteers. As Ms. McDonald mentioned, all analysts are special constables.

Senator Angus: Do your 40 employees work in one place?

Ms. McDonald: We are headquartered in Winnipeg, Manitoba, and we have a Toronto office as well.

Senator Angus: What is your budget?

Ms. McDonald: Our full operating budget is approximately \$4 million, with roughly 97 per cent going to direct programming.

Senator Angus: Without going into a lot of detail, are the people who produce that \$4 million the same people that you thank in your paper for being supporters and sponsors or do you have four main ones?

Ms. McDonald: We have diversified funding. The Government of Canada supplies roughly \$1.7 million annually to operate Cybertip.ca. We raise the balance of the budget through private sector and charitable donations. Including the telcos, we have the banking industry, heating companies and any other corporate groups that want to support our cause.

Senator Angus: Where did the initiative to start this, as you described in 2002, come from?

Ms. McDonald: Our organization was established in 1985 after the abduction and murder of a 13-year-old girl named Candace Derksen. The trial of the individual who allegedly committed that crime is currently ongoing. We recognized the changing face of missing children because of Internet luring, so we set up Cybertip.ca in conjunction with partners to address this growing issue.

Senator Angus: Do you mean yourself? The federal government did not suggest that someone set this up. Rather, a group of concerned parents and citizens set this up.

Ms. McDonald: Yes, it was a group of concerned people that were part of our board structure and organization who initially established the organization.

Senator Angus: I could go on forever. This is a tremendous organization. Where do we send our cheque?

Ms. McDonald: Thank you.

Mme Arnason : Il y a sept analystes et quatre membres du personnel technique ainsi que moi, la directrice, qui travaillent sur la ligne d'assistance. Notre organisation a au total 40 employés. Pour ce qui est de la ligne d'assistance, nous n'avons pas de bénévole. Comme Mme McDonald l'a mentionné, tous les analystes sont des agents de police spéciaux.

Le sénateur Angus : Vos 40 employés travaillent-ils au même endroit?

Mme McDonald : Notre siège social est à Winnipeg, au Manitoba, et nous avons également un bureau à Toronto.

Le sénateur Angus : Quel est votre budget?

Mme McDonald : Notre budget opérationnel s'élève au total à près de quatre millions de dollars, dont 97 p. 100 environ sont utilisés pour la programmation directe.

Le sénateur Angus : Sans aller dans les détails, j'aimerais savoir si les personnes qui sont à l'origine de ce budget de 4 millions de dollars sont les mêmes que celles que vous remerciez dans votre étude, parce qu'ils sont des commanditaires ou des gens qui vous appuient financièrement, ou avez-vous quatre principales sources de financement?

Mme McDonald : Notre financement est très diversifié. Le gouvernement du Canada fournit environ 1,7 million de dollars par an pour le fonctionnement de Cyberaide.ca. Nous recevons le reste du budget sous la forme de dons du secteur privé ou d'organismes de charité. Avec les télécommunications, nous avons le secteur bancaire, les entreprises de chauffage et d'autres sociétés qui appuient financièrement notre cause.

Le sénateur Angus : D'où est venue l'initiative de lancer cette organisation, comme vous l'avez décrit en 2002?

Mme McDonald : Notre organisation a été créée en 1985 après l'enlèvement et le meurtre d'une fille de 13 ans appelée Candace Derksen. L'individu dont il est allégué qu'il a commis ce crime, subit actuellement son procès. Nous savons que le problème des enfants manquants a évolué à cause du leurre sur Internet, et c'est pourquoi nous avons mis sur pied Cyberaide.ca avec des partenaires pour lutter contre ce phénomène en pleine croissance.

Le sénateur Angus : Vous voulez dire vous-même? Ce n'est pas le gouvernement fédéral qui a demandé à quelqu'un de créer cet organisme. C'est plutôt un groupe de parents et de citoyens concernés qui l'a fait.

Mme McDonald : Oui, c'est un groupe de personnes concernées qui faisaient partie de notre organisation et de notre structure administrative qui a mis sur pied au départ l'organisation.

Le sénateur Angus : Je pourrais poursuivre longtemps. C'est une organisation vraiment incroyable. À qui pouvons-nous envoyer notre chèque?

Mme McDonald : Merci.

[Translation]

Senator Boisvenu: So you are working with all the provinces.

[English]

Do you have the data for the province? Is it possible to have that?

Ms. McDonald: We have a statistical sheet in our material.

The Chair: There is a lot of material, so it is probably in here.

Senator Angus: It is there; I saw it.

Ms. McDonald: Anyway, we can read it out. We track —

[Translation]

The Chair: Senator Boisvenu, it is at the end of this document.

Senator Boisvenu: Thank you very much, Madam Chair.

Senator Carignan: Further to Senator Angus's questions on funding, I understand that there are organizations that will fund the centre. I understand that Rogers and Telus are businesses, service providers, that fund the centre. If the centre becomes a designated organization under the act, will it provide for protection to prevent conflicts of interest because, if the business that is being monitored funds the agency, there are significant risks, or at least apparent ones?

[English]

Ms. McDonald: Yes, that is an excellent question. One of the very insightful steps that our organization took when we were established was that no individual could sit on the board of directors if they gave any financial contribution to the organization. That limits the influence over the guidelines and policies of the organization. I can even give examples whereby we had to take steps just to be prudent, even though there was no influence. Additionally, through the establishment of our financial and governing controls, we have independent finance and audit committees that have established clear grounds in terms of our conflicts of interest.

I can also tell you that, when we look at the allocation of funds contributed from these organizations, we allocate those funds directly into public awareness. Therefore, their investment is going directly back into the community to educate the Canadian public.

We would be happy to provide to you a number of those very direct, overt checkpoints that our organization has prudently put in place to separate and make sure there is no conflict.

[Français]

Le sénateur Boisvenu : Vous travaillez donc avec toutes les provinces.

[Traduction]

Avez-vous les données pour la province? Est-il possible de les obtenir?

Mme McDonald : Il y a une feuille de données statistiques dans nos documents.

La présidente : Il y a beaucoup de documents, elle se trouve probablement dans le paquet.

Le sénateur Angus : Elle est là, je l'ai vue.

Mme McDonald : De toute façon, nous pouvons la lire. Nous suivons...

[Français]

La présidente : Sénateur Boisvenu, c'est à la fin de ce document.

Le sénateur Boisvenu : Merci beaucoup, madame la présidente.

Le sénateur Carignan : À la suite des questions du sénateur Angus par rapport au financement, je crois comprendre qu'il y a des organismes qui vont financer le centre. Je crois comprendre que Rogers et Telus sont des entreprises, des fournisseurs de services qui financent le centre. Si le centre devient un organisme désigné en vertu de la loi, est-ce qu'il va prévoir des protections pour éviter les conflits d'intérêts parce que si l'entreprise qu'on surveille finance l'organisme, il y a des risques importants, en apparence en tout cas?

[Traduction]

Mme McDonald : Oui, c'est une excellente question. Notre organisme a pris une mesure très sage lorsqu'il a été créé; il a adopté comme règle que les personnes qui accordent un soutien financier à l'organisation ne peuvent pas être membres du conseil d'administration. Cela limite les influences qui pourraient s'exercer sur les lignes directrices et les politiques de l'organisation. Je peux même vous donner des exemples de mesures que nous avons prises, simplement pour être prudents, même s'il n'y avait aucune possibilité d'influence. En outre, nous avons mis sur pied des mécanismes de contrôle financier et de gouvernance et nous avons des comités de vérification et de finances indépendants qui ont adopté des règles claires en matière de conflits d'intérêts.

Je peux également vous dire que, lorsque nous recevons des fonds de la part de ces organismes, nous les affectons directement à nos campagnes de sensibilisation du public. Ces investissements retournent donc directement dans la collectivité pour informer le public canadien.

Nous serions heureux de vous fournir une liste de ces mécanismes de contrôle très directs et très clairs que notre organisme a mis en place pour séparer ces choses et veiller à ce qu'il n'y ait pas de possibilités de conflit.

[Translation]

Senator Carignan: My other question concerns the police departments. An international convention on cybercrime in Europe was signed in April 2010 and covers the European countries. Australia has suggested the idea of joining that convention to establish an international legislative framework on a common basis to achieve the common objective of all the countries.

To your knowledge, has Canada signed or expressed any intention to join this convention, and, if not, is the legislative process we are currently conducting nevertheless consistent with the spirit of this global legislative framework for the protection of children?

[English]

Mr. Naylor: I am not aware of the framework at the international level or what our partners in Europe are doing with respect to similarities with this legislation. I cannot answer that; I do not know.

[Translation]

Senator Carignan: Can any other members answer that question?

[English]

Mr. Westwick: I am afraid I cannot add much either.

Ms. McDonald: I can mention that there is another charitable organization out of Washington called the International Centre for Missing and Exploited Children. They publish a report ranking countries and looking specifically at how they are addressing the issue of child pornography.

I would have to verify this information. However, should this bill move forward, I believe Canada would be 1 of 9 countries out of over 100 countries that would be meeting these high criteria for good practice.

[Translation]

Senator Carignan: The duty to preserve computer data. I get the impression that may be inadequate in certain situations. Consider the example of an ISP that, for example, is a hotel or a restaurant; protecting computer data is one thing, but there may be information, not in a digital medium, but that should be preserved in order to identify the user of the computer terminal. When you go to a hotel, you get an access code and you access the Internet service. However, the paper document or bill, which links the individual to the access code, is an example of a piece of paper that might be useful in the context of an investigation. I am trying to imagine; there are no doubt others.

Do you think the bill goes far enough with other information that might help identify a suspicious user?

[Français]

Le sénateur Carignan : Mon autre question concerne les services policiers. Il y a eu une convention internationale en Europe sur la cybercriminalité, qui a été signée en avril 2010, et qui couvre les pays européens. L'Australie a manifesté l'idée de se joindre à cette convention pour créer un cadre législatif international qui puisse avoir des bases semblables pour atteindre l'objectif commun visé par tous les pays.

À votre connaissance, est-ce que le Canada a signé ou manifesté l'intention de participer à cette convention et sinon, est-ce que le processus législatif qu'on effectue actuellement entre quand même dans l'esprit de ce cadre législatif mondial pour la protection des enfants?

[Traduction]

M. Naylor : Je ne connais pas le cadre qui existe au palier international ni ce que font nos partenaires en Europe à l'égard de mesures semblables à ce projet de loi. Je ne peux pas répondre à cette question; je ne sais pas.

[Français]

Le sénateur Carignan : Est-ce que d'autres membres peuvent répondre à cette question?

[Traduction]

M. Westwick : Je suis désolé, mais je ne peux pas ajouter grand-chose non plus.

Mme McDonald : Je peux mentionner qu'il existe un autre organisme de charité qui est basé à Washington et qui s'appelle l'International Centre for Missing and Exploited Children. Il publie un rapport où les pays sont classés en fonction de la façon dont ils abordent la lutte contre la pornographie juvénile.

Il faudrait que je vérifie cette information. De toute façon, si ce projet de loi est adopté, je pense que le Canada sera un des 9 pays, sur plus de 100 pays, qui sont en mesure de répondre à ces critères exigeants en matière de bonne pratique.

[Français]

Le sénateur Carignan : L'obligation est de préserver les données informatiques. J'ai l'impression que cela peut être insuffisant dans certaines situations. Je vous donne l'exemple du FSI qui serait, par exemple, un hôtel ou un restaurant, de protéger les données informatiques, c'est une chose. Mais il peut y avoir de l'information non pas sur support informatique, mais qui devrait être conservé pour identifier l'utilisateur du poste informatique. Quand on va à l'hôtel, on reçoit un code d'accès et on accède au service Internet. Mais le document ou la facture de support papier, qui fait le lien entre l'individu et le code d'accès, est un exemple de papier qui pourrait être utile dans le cadre d'une enquête. J'essaie d'imaginer, il y en a sûrement d'autres.

Est-ce que vous pensez que le projet de loi va assez loin et qu'on ne devrait pas élargir à d'autres informations qui pourraient permettre d'identifier un utilisateur suspect?

The Chair: Minor technical question.

[English]

Mr. Naylor: I think the bill is sufficient in the way that it is written, including the 21 days. This does not include completing the investigation; it is just to launch the investigation. There are several investigative steps that need to be completed by the police. Having had experience in this, it is my opinion that 21 days from the time of the report is sufficient enough to obtain any type of judicial authorization in a matter of this serious nature.

Mr. Westwick: As I said in my opening remarks, it is a lead or starting point. As the inspector said, it is not the whole investigation. It is to get the file open, to get movement, to get started and to get information that the police might not otherwise get.

[Translation]

Senator Chaput: My first question is for Ms. McDonald. Cybertip.ca is a Canadian national tipline for reporting sexual exploitation cases. When I read that you receive an average of 700 reports a month and 75,000 interventions a month, I wonder how many of those reports come from outside Canada and how many must be forwarded outside Canada.

[English]

Ms. Arnason: I will answer that question. The vast majority come from Canadians, although we do have other countries, such as the United States, coming to us and reporting. I do not have that exact figure in front of me.

However, as it relates to where we forward information, I can tell that you 82 per cent of our reports that come in end up going outside of Canada. That means that 18 per cent are forwarded to the appropriate Canadian law enforcement jurisdiction.

[Translation]

Senator Chaput: Are you responsible for ensuring that something is done with the reports sent outside Canada, or is it no longer your responsibility to ensure that something is done once it leaves the country?

[English]

Ms. Arnason: We work very closely under the national strategy with the National Child Exploitation Coordination Centre out of Ottawa. It is run by the RCMP. They are our partners that receive any of the information that ends up going internationally. They come in through a law enforcement portal to provide feedback on

La présidente : Petite question technique !

[Traduction]

M. Naylor : Je crois que le projet de loi est suffisant, sous sa forme actuelle, y compris la période de 21 jours. Il n'est pas nécessaire d'achever l'enquête à l'intérieur de cette période; il suffit simplement de la lancer. La police doit prendre une série de mesures dans le cadre de ce genre d'enquête. J'ai de l'expérience dans ce domaine et j'estime qu'une période de 21 jours à partir du signalement est suffisamment longue pour que la police puisse obtenir une autorisation judiciaire lorsque l'affaire est grave.

M. Westwick : Comme je l'ai dit dans mes remarques d'ouverture, c'est une piste ou un point de départ. Comme l'a dit l'inspecteur, cela ne recouvre pas toute l'enquête. Il s'agit d'ouvrir un dossier, de démarrer les choses, de commencer et d'obtenir l'information que la police n'obtiendrait peut-être pas autrement.

[Français]

Le sénateur Chaput : Ma première question est pour Mme McDonald. Cyberaide.ca est une ligne canadienne nationale de signalement des cas d'exploitation sexuelle. Lorsque je lis que vous recevez en moyenne 700 signalements par mois, et 75 000 interventions par mois, combien de ces signalements proviennent de l'extérieur du Canada et combien de ces signalements doivent être transmis à l'extérieur du Canada?

[Traduction]

Mme Arnason : Je veux répondre à cette question. L'immense majorité des signalements viennent des Canadiens, même s'il y a d'autres pays, comme les États-Unis, qui s'adressent à nous pour nous communiquer des signalements. Je n'ai pas le chiffre exact avec moi.

Cependant, pour ce qui est des organismes à qui nous transmettons ces renseignements, je peux vous dire que 82 p. 100 des signalements que nous recevons sont redirigés vers l'étranger. Cela veut dire que 18 p. 100 seulement sont transmis aux autorités canadiennes compétentes en matière d'application de la loi.

[Français]

Le sénateur Chaput : Avez-vous la responsabilité de vous assurer que quelque chose est fait avec les signalements envoyés à l'extérieur du Canada ou est-ce qu'au moment où c'est parti, ce n'est plus votre responsabilité de vous assurer que quelque chose soit fait?

[Traduction]

Mme Arnason : Nous travaillons en étroite collaboration, dans le cadre de la stratégie nationale, avec le Centre national de coordination contre l'exploitation des enfants d'Ottawa. Il est administré par la GRC. Ce sont nos partenaires qui reçoivent les renseignements qui sont finalement destinés à l'étranger. Nous les

any potential results. It is my understanding that they take that information and forward it through Interpol, then follow up on that.

Ms. McDonald: It is important to note that our organization is not an investigative body. Our job is to triage the information for forwarding. It is up to the appropriate law enforcement agency to decide on further investigative action should any be taken.

[Translation]

Senator Chaput: My next question is for Inspector Naylor.

[English]

I am told that there is a centralized database that allows the RCMP to share information with 25 Canadian police forces.

Mr. Naylor: Yes.

Senator Chaput: I believe that in your presentation you talked about returned predators. Does the centralized database contain a list of the names of predators that offended and have re-offended so that you can be aware of what is going on? When a predator is released from prison, is his name removed from the database?

Mr. Naylor: No. The name always stays in the database.

Senator Chaput: The name is like a red flag.

Mr. Naylor: It is a red flag. However, our investigations are mostly reactive, so we have to wait for someone to offend in order to compare that name and IP address to the person on the list. There is no ankle bracelet or anything like that for us to monitor those people on a regular basis. We have to wait for them to fall into our net again. We maintain a database of previously convicted criminals.

Senator Chaput: Who pays the bill for that?

Mr. Naylor: The RCMP.

Senator Chaput: What is the role of Microsoft? Do they only sell the service?

Mr. Naylor: No. They do not even sell the service. Microsoft has donated the service and the RCMP is responsible for maintaining the database. It is called CETS, child exploitation tracking system.

Senator Runciman: My first question is to Inspector Naylor about the 21-day preservation period. You may have heard the previous witness indicate that she felt the timeline was too long.

obtenons par un portail d'application de la loi qui nous fournit des commentaires sur les résultats obtenus. Je crois savoir qu'ils prennent ces renseignements et les transmettent à d'autres organismes par Interpol, et qu'ils font ensuite un suivi.

Mme McDonald : Il est important de noter que notre organisation ne s'occupe pas de faire des enquêtes. Notre rôle consiste à trier les renseignements que nous recevons pour les transmettre ensuite. Il appartient alors à l'organisme d'application de la loi compétent de décider dans chaque cas s'il y a lieu de lancer une enquête.

[Français]

Le sénateur Chaput : Ma prochaine question s'adresse à l'inspecteur Naylor.

[Traduction]

On m'a dit qu'il existe une base de données centralisée qui permet à la GRC de partager des renseignements avec 25 services de police canadiens.

M. Naylor : Oui.

Le sénateur Chaput : Je crois que vous avez parlé dans votre exposé des prédateurs récidivistes. Est-ce que la base de données centralisée contient une liste des noms des prédateurs qui ont commis une infraction et récidivé ensuite, pour que vous puissiez savoir ce qui se passe? Lorsqu'un prédateur est libéré de prison, son nom est-il supprimé de la base de données?

M. Naylor : Non. Le nom reste toujours dans la base de données.

Le sénateur Chaput : Le nom est donc comme un signal d'alarme.

M. Naylor : C'est un signal d'alarme. Normalement, nous ne déclençons une enquête que lorsque nous recevons des renseignements au sujet d'une infraction, de sorte que nous devons attendre que quelqu'un en commette une pour pouvoir comparer ce nom et l'adresse IP avec ceux de la personne sur la liste. Il n'y a pas de bracelet émetteur ou de chose de ce genre qui nous permette de suivre régulièrement ces personnes. Nous devons attendre qu'elle retombe dans nos filets. Nous conservons une base de données des délinquants ayant été condamnés.

Le sénateur Chaput : Qui paie les frais de tout ceci?

M. Naylor : La GRC.

Le sénateur Chaput : Quel est le rôle de Microsoft? Cette entreprise vend-elle uniquement le service?

M. Naylor : Non. Cette société ne vend même pas le service. Microsoft a fait don du service et la GRC est chargée de s'occuper de la base de données. Cela s'appelle le système d'analyse contre la pornographie juvénile, le CETS d'après le nom en anglais.

Le sénateur Runciman : Ma première question s'adresse à l'inspecteur Naylor et porte sur la période de préservation de 21 jours. Vous avez peut-être entendu le témoin précédent

Another witness said they could use additional time. Could you give us a quick overview of what happens during that period of time?

Mr. Naylor: Yes. Having had experience in this through several areas of law enforcement, as soon as it comes to the attention of law enforcement that there is an offence and that some form of judicial authorization is required to obtain a search warrant and information, a relationship is made with whomever is holding that information. Specifically, that means the 21-day legislative requirement in the bill becomes a bit of a moot point because the law enforcement officer and the person holding the information have already established that relationship. Once that relationship is established, there can be communication between the two, such as the law enforcement officer saying that his search warrant is coming today or in three days.

I do not want to get handcuffed — pardon the pun — by the 21-day period. It is most important to law enforcement that the information lands in their lap so that we can take action. I believe the 21 days is sufficient but not ideal. When we are dealing with issues of such a serious nature, they cannot be put on the back burner; they need to be acted upon immediately.

Senator Runciman: Senator Munson was here earlier. His comments in the Senate expressed concern about the two-step process in the bill. Would any of the witnesses care to speak to that?

Ms. McDonald: My comment at the beginning was that the bill addresses the two complexities of Internet-facilitated crimes against children. We have websites that propagate crime. Often they are hosted outside Canada. This is the bulk of the reporting that we receive. Law enforcement should spend their time working on investigations that deal with actual offenders. The second part of the bill deals with material that can be found on an Internet service. This adequately allows police to address that issue, which makes good sense.

It is difficult to understand and appreciate fully how this happens on the Internet but the bill wisely, in our opinion, addresses these two complexities.

Senator Runciman: You validate the seriousness and then pass it on to the police if it has merit and requires that further step.

Ms. McDonald: Yes.

Senator Runciman: You mentioned in your submission as well that 80 per cent of the content is hosted outside Canada. Do you know how much of it is produced in Canada?

Ms. McDonald: No.

déclarer qu'elle estimait que cette période était trop longue. Un autre témoin nous a dit qu'il serait bon d'allonger cette période. Pourriez-vous nous donner un bref aperçu de ce qui se passe pendant cette période?

M. Naylor : Oui. J'ai de l'expérience dans ce domaine parce que j'ai travaillé dans plusieurs secteurs de l'application de la loi, et dès qu'un organisme de l'application de la loi apprend qu'une infraction a été commise et qu'il faut obtenir une autorisation judiciaire pour se procurer un mandat de perquisition et déposer une dénonciation, un lien s'établit avec la personne qui détient les renseignements. Plus précisément, cela veut dire que la période de 21 jours prévue par le projet de loi devient un peu théorique parce que l'agent d'application de la loi et la personne qui détient l'information ont déjà établi un lien. Une fois que cette relation est établie, ces deux personnes peuvent communiquer, de sorte que l'agent d'application de la loi peut par exemple dire qu'il obtiendra dans deux ou trois jours son mandat de perquisition.

Je ne veux pas me sentir trop limité par la période de 21 jours. Il est extrêmement important pour les services d'application de la loi que l'information arrive le plus rapidement possible en leur possession pour qu'ils puissent intervenir. Je pense qu'une période de 21 jours est suffisante mais pas idéale. Lorsqu'il s'agit de questions aussi graves, il n'est pas possible de les remettre à plus tard; il faut agir immédiatement.

Le sénateur Runciman : Le sénateur Munson était ici plus tôt. Il a fait des commentaires au Sénat dans lesquels il exprimait être préoccupé par le processus en deux étapes prévu par le projet de loi. Est-ce qu'un des témoins aimerait parler de ce sujet?

Mme McDonald : J'ai dit dans mes commentaires que le projet de loi visait les deux aspects complexes des crimes commis contre les enfants à l'aide d'Internet. Nous avons des sites web qui propagent ce crime. Ils sont bien souvent hébergés à l'extérieur du Canada. C'est à ce sujet que nous recevons la plus grande partie de nos signalements. Les services d'application de la loi devraient consacrer leur temps aux enquêtes concernant des délinquants. La deuxième partie du projet de loi traite du matériel que l'on peut trouver sur Internet. Cela est suffisant pour permettre à la police d'intervenir, ce qui est une bonne chose.

Il est difficile de comprendre vraiment comment cela se passe sur Internet, mais je dirais que d'après nous, le projet de loi aborde, de façon très sage, ces deux aspects complexes.

Le sénateur Runciman : Vous vérifiez la gravité du signalement et le transmettez ensuite à la police si celui-ci est fondé et exige que l'on passe à une autre étape.

Mme McDonald : Oui.

Le sénateur Runciman : Vous avez également mentionné dans votre exposé que 80 p. 100 de ce contenu est hébergé à l'extérieur du Canada. Savez-vous quel pourcentage de ce contenu est produit au Canada?

Mme McDonald : Non.

Senator Runciman: I ask that because last summer there was a worldwide investigation and 57 men were charged, including 25 Canadians. Almost 50 per cent were Canadians, which would suggest that it is a pretty serious problem in Canada. Do you have any further information on that?

Ms. McDonald: No. Certainly, Inspector Naylor can speak to individuals and arrests pertaining to those committing these types of crimes, but we want to underscore that our goal is to consider that we want to stop the images from getting on the Internet in the first place. The goal is to stop the sexual abuse in homes and communities before the photography takes place and ends up online. We are hoping that this bill will provide law enforcement with the information required to stop hands-on offenders.

Senator Runciman: I have two quick questions.

The Chair: Senator Joyal is waiting and I am waiting, actually.

Senator Runciman: Inspector Naylor, how do you go about identifying and rescuing the victims?

Mr. Naylor: In most circumstances, the victims rescued are familial victims of the people under arrest. With respect to some of these bigger projects, such as Project Sanctuary, many of the victims are family members and that is how they are identified.

Senator Runciman: Mr. Westwick, concern was expressed by someone who made a submission about the interpretation of “reasonable grounds to believe.” How do you see that applying? Do you see that as a concern?

Mr. Westwick: Not at all. In the policing world, reasonable grounds to believe is something that people will deal with from their first day on the job, even before they go on the job. The concept is certainly familiar within the law enforcement world. I do not think it would present a great deal of difficulty for the ISPs. I cannot imagine that it will be a difficulty.

Senator Runciman: Does it put them under any legal jeopardy that you can see?

Mr. Westwick: I cannot imagine so.

Senator Joyal: Ms. McDonald, on your opening page you mention that you have received nearly 52,000 reports from the public. Can you give us an idea how many of those reports would not lead to a report to police because you judge them not to be serious in nature? Can you give us an idea of the right stuff and what is nothing to be concerned about?

Ms. Arnason: As mentioned, 40 per cent of the information that comes into the tip line is forwarded to the appropriate law enforcement jurisdiction, which means that 54 per cent of the information does not go to law enforcement so they do not have

Le sénateur Runciman : Je pose la question parce qu’il y a eu l’été dernier une enquête internationale qui a débouché sur l’inculpation de 57 hommes dont 25 étaient des Canadiens. Près de 50 p. 100 étaient des Canadiens, ce qui semble indiquer que la situation est très grave au Canada. Avez-vous d’autres renseignements sur cette affaire?

Mme McDonald : Non. Je suis sûre que l’inspecteur Naylor peut parler des personnes et des arrestations reliées à ce genre de crimes, mais nous tenons à souligner que notre objectif est de faire en sorte que les images ne se rendent pas sur Internet au départ. L’objectif est de mettre un terme aux agressions sexuelles commises dans les maisons et dans les collectivités avant que la photographie soit prise et se retrouve en ligne. Nous espérons que ce projet de loi donnera aux services d’application de la loi l’information dont ils ont besoin pour arrêter les délinquants.

Le sénateur Runciman : J’ai deux brèves questions.

La présidente : Le sénateur Joyal attend et j’attends également, en fait.

Le sénateur Runciman : Inspecteur Naylor, comment faites-vous pour identifier et sauver les victimes?

M. Naylor : Dans la plupart des cas, les victimes que nous sauvons sont des membres de la famille des personnes arrêtées. Pour ce qui est de certains grands projets, pour le Project Sanctuary, la plupart des victimes étaient des membres de la famille et c’est ainsi qu’elles ont été identifiées.

Le sénateur Runciman : Monsieur Westwick, quelqu’un a déclaré être préoccupé par l’interprétation de l’expression « motifs raisonnables de croire. » Comment pensez-vous que cette expression sera appliquée? Pensez-vous qu’elle fera problème?

M. Westwick : Pas du tout. Dans le monde de la police, la notion de motifs raisonnables de croire est une notion que les agents appliquent dès leur premier jour de travail, même avant qu’ils commencent leur travail. Cette notion est très courante dans le milieu de l’application de la loi. Je ne pense pas qu’elle représenterait une grande difficulté pour les FSI. Je ne peux pas imaginer que cela pose un problème.

Le sénateur Runciman : Est-ce que cela risque de les placer en danger sur le plan juridique, d’après vous?

M. Westwick : Je ne peux l’imaginer.

Le sénateur Joyal : Madame McDonald, vous mentionnez dans votre première page que vous avez reçu près de 52 000 signalements de la part du public. Pouvez-vous nous donner une idée du nombre de ces signalements qui ne débouchent pas sur un signalement à la police, parce que vous estimez qu’ils ne sont pas suffisamment graves pour le faire? Pouvez-vous nous donner une idée de ce qui est grave et des choses dont il n’est pas nécessaire de se préoccuper?

Mme Arnason : Comme cela a été mentionné, 40 p. 100 des renseignements qui arrivent à la ligne d’assistance sont transmis aux services d’application de la loi compétents, ce qui veut dire que 54 p. 100 des renseignements ne sont pas transmis à ces

to process the information. That is because it is clearly legal. Anything that is potentially legal or grey, we leave in the hands of law enforcement to determine whether they will take action from an investigative standpoint. We get a number of Canadians coming in and reporting adult pornography. It is highly offensive and egregious to the individual and can border on obscenity, but it is legal. That kind of information is triaged by us and, in some instances, hits an educational track as well.

Mr. Naylor: As a recipient of this from Cybertip, Cybertip works on the same basis that we do for categorization of images, and they are spot on. If there is ever any question, then they default to the less severe to send to law enforcement for analysis.

Ms. McDonald: I would like to add to some of the earlier comments made. We dealt with this when contemplating mandatory reporting in Manitoba. Even though people come forward and it increases workloads, reporting does not equate guilt. When we are looking at children and as we explore this, we are simply giving children added protection. As mentioned, the reporting itself can assist in the detection of abuse and the identification of possible offenders.

Senator Joyal: In other words, a little more than 50 per cent of the reporting is not stuff that would be followed up on in terms of child pornography.

Ms. McDonald: That is correct.

Senator Joyal: My other preoccupation about this hopefully effective bill is the additional workload that it will put either on the police forces or on your own services. We were told by the federal ombudsman that there is a serious backlog — that the current backlog that many law enforcement agencies face in investigating these cases is due to a lack of resources and manpower. One could expect that, if this bill is implemented, you would have an additional workload; there would be more reports to investigate and, of course, more initiative to be taken by you.

How would you deal with this additional work you may have to face if you already have a backlog?

Mr. Naylor: There is a huge proliferation of child pornography on the Internet. If I had 100 people in my unit, I would need 200. We will not catch up to this. However, we have to take every possible step we can to effectively enforce and investigate any report of child pornography. Investigators in Ontario look at it by thinking that there is a potential live victim at the other end of the Internet; it is our responsibility to at least fully investigate to see if we can get that child out of a dangerous situation.

services qui n'ont donc pas à les examiner. C'est parce que la situation signalée est parfaitement légale. Tout ce qui risque d'être illégal ou qui entre dans une zone grise est remis entre les mains des services d'application de la loi pour qu'ils décident eux-mêmes s'il y a lieu d'intervenir et de lancer une enquête. Il y a un certain nombre de Canadiens qui nous signalent de la pornographie pour adultes. Elle est très choquante et très préjudiciable à la personne qui la subit, elle peut même être à la limite de l'obscénité, mais elle est légale. Nous faisons le tri de cette information et dans certains cas, nous l'intégrons à nos programmes d'information.

M. Naylor : En tant que destinataire des renseignements provenant de Cyberaide, je dirais que Cyberaide travaille de la même façon que nous le faisons pour classer les images et cet organisme ne se trompe pas. S'il se pose des questions, alors il s'en remet aux analystes des services d'application de la loi.

Mme McDonald : J'aimerais ajouter quelque chose à des commentaires que j'ai faits plus tôt. Nous avons abordé cette question lorsque nous avons envisagé le signalement obligatoire au Manitoba. Même si les gens n'hésitent pas à communiquer ce qu'ils savent et que cela augmente les charges de travail, ces signalements ne déboucheront pas tous sur des déclarations de culpabilité. Si nous pensons aux enfants pendant que nous explorons ces aspects, il s'agit simplement de mieux protéger les enfants. Comme cela a été mentionné, les signalements peuvent faciliter la détection des agressions et l'identification des délinquants.

Le sénateur Joyal : Autrement dit, un peu plus de 50 p. 100 des signalements ne donnent pas lieu à un suivi sur le plan de la pornographie juvénile.

Mme McDonald : C'est exact.

Le sénateur Joyal : L'autre aspect de ce projet qui sera, je l'espère, efficace, et qui me préoccupe est qu'il va ajouter une charge de travail supplémentaire soit aux forces de police, soit à vos propres services. L'ombudsman fédéral nous a dit qu'il y avait un arriéré important — que l'arriéré actuel qui existe dans de nombreux services d'application de la loi est dû à un manque de ressources et de personnel, ce qui ralentit les enquêtes dans ce genre d'affaires. On pourrait s'attendre à ce que, si le projet de loi est mis en œuvre, votre charge de travail augmente; vous allez devoir faire enquête sur davantage de signalements et, bien entendu, prendre davantage d'initiatives.

Comment allez-vous faire pour exécuter ce travail supplémentaire si vous avez déjà un arriéré?

M. Naylor : La pornographie juvénile sur Internet se multiplie très rapidement. Si j'avais 100 personnes dans mon unité, j'en aurais besoin de 200. Nous n'arriverons jamais à rattraper ce retard. Nous devons toutefois faire tout ce qui est possible pour faire enquête sur tous les signalements de pornographie juvénile. En Ontario, les enquêteurs considèrent qu'il y a une victime qui est peut-être encore vivante à l'autre bout d'Internet; notre responsabilité consiste au moins à faire une enquête approfondie pour voir si nous pouvons retirer cet enfant de la situation dangereuse dans laquelle il se trouve.

I do not know if I am answering your question about manpower. We do the best we can with what we have. We do the best we can within our budget allocations. I feel this is good legislation in order to bring more reports to law enforcement in order to effectively investigate.

Senator Joyal: However, at this stage, you have not set aside an additional amount for more investigators, policemen or for Ms. McDonald's services to have additional people to be able to process more reports that come to you; is that correct?

Ms. Arnason: In the last 10 years, we have developed an expertise in doing the up-front triaging. We employ a number of technical solutions to ensure the information, particularly websites, are dealt with expeditiously. We know that the mass majority of these websites, which we are obviously dealing with under this bill, will be forwarded internationally.

For example, there may be a slight increase to Canadian law enforcement. However, if you are looking at Ontario, we have had 5,800 websites reported to us since April 2008. That has resulted in 263 going to an Ontario law enforcement agency. Therefore, 4.5 per cent of what came to us from Ontario went into Ontario.

Again, it is the value of triaging, recognizing that a lot of this content is hosted internationally, and knowing that we have spent the last 10 years triaging website content. I do not have any significant concerns about our ability to manage that.

Senator Joyal: Someone at the "end of the rope" will have to deal with that information. I do not doubt you have the capacity because you have developed a scale of analysis that permits you to decide or classify which cases are child pornography and which are not. However, at the other end, Mr. Naylor and Mr. Westwick will have to deal with additional investigations if this bill is to reach its objective.

Mr. Naylor: There is the potential that some of the information we receive from ISPs would have been received later through a full investigation, anyway.

Senator Joyal: It could also be done by going to court to get a warrant. We were told that 30 per cent to 40 per cent of Internet service providers do not comply spontaneously. They give the information if it is requested under a court warrant.

Mr. Westwick: There is not a chief of police in the country who would not be happy to have the resources, but there is also not a chief of police in the country who is not dealing with budgetary constraints and pressures.

Je ne sais pas si je réponds à votre question sur le personnel. Nous faisons du mieux que nous pouvons avec ce que nous avons. Nous faisons ce que nous pouvons avec notre budget. J'estime qu'il s'agit là d'un bon projet de loi qui va augmenter le nombre des signalements transmis aux agences d'application de la loi qui pourront alors faire enquête.

Le sénateur Joyal : Toutefois, vous n'avez pas encore mis de côté une somme supplémentaire pour embaucher d'autres enquêteurs, d'autres policiers ou pour que les services de Mme McDonald puissent avoir du personnel supplémentaire qui pourra traiter les signalements qui vous seront transmis, est-ce bien exact?

Mme Arnason : Au cours des 10 dernières années, nous avons acquis de l'expertise pour ce qui est du tri de première ligne. Nous avons recours à un certain nombre de solutions techniques pour veiller à ce que l'information, en particulier celle qui concerne les sites web, soit traitée rapidement. Nous savons que l'immense majorité des sites web, et ce sont eux qui sont visés par le projet de loi, se trouvent à l'étranger.

Par exemple, il se pourrait que les services d'application de la loi du Canada enregistrent une légère augmentation de ces cas. Cependant, en Ontario, nous avons reçu 5 800 signalements de sites web depuis avril 2008. De ce nombre, 263 ont été transmis aux agences d'application de la loi de l'Ontario. Quatre et demi pour cent des signalements provenant de l'Ontario ont été transmis à des services de l'Ontario.

Encore une fois, c'est toute l'utilité du tri; il faut savoir qu'une bonne partie de ce contenu est hébergée à l'étranger et que nous avons consacré les 10 dernières années à trier le contenu de sites web. Je n'ai aucune inquiétude au sujet de notre capacité à gérer cela.

Le sénateur Joyal : Quelqu'un en bout de ligne sera bien obligé de traiter cette information. Je ne doute pas que vous ayez cette capacité, parce que vous avez mis sur pied un type d'analyse qui vous permet de trier ou de classer les affaires qui constituent de la pornographie juvénile et celles qui n'en sont pas. Cependant, à l'autre extrémité, M. Naylor et M. Westwick seront obligés d'effectuer davantage d'enquêtes si le projet de loi atteint son objectif.

M. Naylor : Il est possible que nous aurions obtenu de toute façon au cours de notre enquête les renseignements que les FSI vont nous fournir.

Le sénateur Joyal : Nous pourrions aussi y parvenir en demandant un mandat à un tribunal. On nous a dit que 30 à 40 p. 100 des fournisseurs de services Internet ne collaboraient pas spontanément. Ils fourniront ces renseignements si une ordonnance de la Cour les oblige à le faire.

M. Westwick : Il n'y a pas un seul chef de police au Canada qui ne serait pas heureux d'avoir davantage de ressources, mais il n'y a pas un seul chef de police au Canada qui ne connaît pas de difficultés financières.

What it forces police services to do is be smarter. You have had a couple of examples at this table of how that is being done. You are seeing more cooperation between municipal, provincial and federal police services. You are seeing community partnerships being used. You are also seeing civilianization of police positions, where possible, so they can be more economical and smarter in how they use the budget they have.

More money and more people is not always the answer. Chiefs of police have had to find ways to be creative to get the job done. That is what makes their job tough, I am afraid.

The Chair: We are into overtime. I am giving up my own question so that you can have one more.

Senator Joyal: I can conclude quickly. At this stage, you do not have a decision that, if this bill is implemented, you will have X amount of people or officers devoted to be able to deal with the additional reports that deserve investigations; is that correct?

Mr. Naylor: No. However, we can re-prioritize some of the proactive investigations we do to address the reactive ones we will get from this reporting legislation.

The Chair: Thank you. You can tell that we actually could have kept any one of you here for a lot longer, let alone all three groups. We are very grateful for your help and for all the material you have provided.

[Translation]

Senator Boisvenu, I misled you earlier. My provincial statistics are not in the document I referred to.

[English]

I will ask the witness from Cybertip to please forward us the provincial statistics that Senator Boisvenu asked for.

Ms. McDonald: We will do so immediately. We brought some other educational materials as well. I know we have loaded you up.

The Chair: Please provide them to the clerk and we will be glad to make them available to the committee.

Colleagues, we are now fortunate to have an expert witness from ExitCertified, Michael MacKay, Senior Consultant. He actually understands how these things work, and he is here to help us understand how these things work. Mr. MacKay, I believe you have a statement for us.

Cela oblige les services de police à agir de façon plus intelligente. On vous a donné quelques exemples de la façon dont cela se fait. Vous pouvez constater que les services de police fédéraux, provinciaux et municipaux collaborent davantage. Vous pouvez voir que nous mettons sur pied des partenariats communautaires. Vous voyez également que certains postes des services de police sont confiés à des civils, lorsque cela est possible, parce que cela est plus économique et permet de mieux utiliser le budget.

Il ne suffit pas toujours d'augmenter les budgets et le personnel. Les chefs de police ont été obligés de trouver des façons créatives de faire leur travail. C'est ce qui rend leur travail difficile, je le crains.

La présidente : Nous avons dépassé le temps prévu. Je renonce à poser ma propre question pour que vous puissiez en poser une autre.

Le sénateur Joyal : Je vais conclure rapidement. À cette étape-ci, vous ne savez pas si, dans le cas où ce projet de loi serait adopté, vous aurez X agents ou employés qui pourront se consacrer aux signalements supplémentaires qui méritent de faire l'objet d'une enquête, est-ce bien exact?

M. Naylor : Non. Nous pouvons toutefois modifier les priorités de certaines enquêtes à but préventif pour nous occuper des enquêtes qui font suite aux signalements prévus par la loi.

La présidente : Merci. Vous avez constaté que nous aurions pu vous garder tous beaucoup plus longtemps, sans parler des trois groupes. Nous sommes très reconnaissants de l'aide vous nous avez apportée et des documents que vous nous avez remis.

[Français]

Sénateur Boisvenu, je vous ai induit en erreur tout à l'heure. Mes statistiques provinciales ne font pas partie du document dont je parlais.

[Traduction]

Je vais demander au témoin de Cyberaide de bien vouloir nous transmettre les statistiques provinciales que le sénateur Boisvenu a demandées.

Mme McDonald : Nous allons le faire immédiatement. Nous avons également apporté d'autres documents d'information. Je sais que nous vous en avons remis beaucoup.

La présidente : Veuillez les remettre à la greffière et nous nous ferons ensuite un plaisir de les distribuer aux membres du comité.

Chers collègues, nous avons maintenant la chance d'entendre un témoin expert d'ExitCertified, Michael MacKay, consultant principal. Il comprend en fait comment fonctionne ce genre de choses et il est ici pour nous aider à comprendre ce qui se passe. Monsieur MacKay, je pense que vous allez nous présenter un exposé.

Michael MacKay, Senior Consultant, ExitCertified: Thank you. Yes, I have prepared a presentation, which I hope the members have had a chance to look at. I would be happy to answer your questions on that. Rather than summarize the presentation, I thought I would, in my brief opening remarks, make a few comments to directly address the issue about how this works. How do web pages work? How do images show up there? What are these things that the bill talks about — Internet protocol, IP, addresses, uniform resource locator — and why is it important that these things in particular be reported?

The whole point is that we all want to see, first, that incidents of child pornography on the Internet do not come about in the first place, and there can be technical means to do that. If they do come about, we would like to isolate them, stop them and ultimately go after the people who put them there. If we are focusing on the Internet aspect, that is what I want to do.

I wanted to take just an example to show the experience of the end user who, let us say, unfortunately becomes the recipient of this offensive and possibly criminal material. Rather than show you that, I decided to show you a very normal looking web page. Do you have this presentation with the first page showing a picture of your own website? I say “your own” because it is the Senate of Canada website.

Senator Angus: Do we have that?

The Chair: We do. It looks like this.

Mr. MacKay: There is a photograph of the building we are in.

The Chair: If you do not have it yet, we will get it to you.

Mr. MacKay: Sorry, it is the Centre Block, a few steps away.

The Chair: Press on, Mr. MacKay.

Mr. MacKay: Thank you. I want to point out, with these few slides, where and how I did this. I did this at home, and I did that because I wanted to show that anyone ordinary could do this. I did not do this at some office or some special computer. This is my home computer on the Internet. Anyone in the world could have done what I am doing right here. Anyone can visit a website if they have an Internet computer with a browser.

This is what I saw in my browser when I visited the Senate of Canada website. This is just the front page. Immediately, you see that image there of the Centre Block. I want to talk about that image. Instead of being this nice photograph, suppose it was something we had a serious concern about.

How did I get here? You will see at the top something called a uniform resource locator. I have circled it there. It is an address. It is the location on the Internet of this page. I got that the way most people do. I went to a search engine like Google. I typed in the

Michael MacKay, consultant principal, ExitCertified : Merci. Oui, j'ai préparé un exposé et j'espère que les membres du comité ont pu en prendre connaissance. Je serai heureux de répondre à vos questions à ce sujet. Plutôt que de résumer mon exposé, j'ai pensé que je vous présenterais, dans mes brèves remarques d'ouverture, quelques commentaires qui portent directement sur le fonctionnement de tout cela. Que sont les pages web? Comment est-ce que les images s'y retrouvent? Quelles sont les choses dont parle le projet de loi — protocole Internet, adresses IP et URL — et les raisons pour lesquelles il est important que ces choses en particulier soient signalées?

La grande question est que nous voulons tous, premièrement, que la pornographie juvénile n'apparaisse pas sur Internet, et il existe des moyens techniques d'y parvenir. Si cette pornographie apparaît, nous aimerions l'isoler, l'arrêter et finalement retrouver les personnes qui l'ont affichée sur Internet. Si nous voulons nous attaquer à l'aspect Internet, c'est ce que je voudrais faire.

Je vais vous donner un exemple pour montrer quelle est l'expérience de l'utilisateur final qui reçoit malgré lui ce matériel choquant et peut-être criminel. Plutôt que de vous montrer ce genre de choses, j'ai décidé de vous montrer une page web tout à fait normale. Avez-vous le document dont la première page montre une image de votre propre site web? Je dis « votre propre site », parce que c'est le site web du Sénat du Canada.

Le sénateur Angus : Est-ce que nous l'avons?

La présidente : Oui. Voilà à quoi il ressemble.

M. MacKay : Il y a une photographie de l'édifice où nous nous trouvons.

La présidente : Si vous ne l'avez pas encore, nous allons vous le faire parvenir.

M. MacKay : Désolé, c'est l'édifice du Centre, à quelques pas d'ici.

La présidente : Poursuivez, monsieur MacKay.

M. MacKay : Merci. Je veux vous montrer, avec ces quelques diapositives, où j'étais quand j'ai fait ce travail et comment je l'ai fait. J'ai fait ça chez moi et je l'ai fait parce que je voulais vous montrer que n'importe qui pouvait le faire. Je n'ai pas fait ce genre de chose dans un bureau ou avec un ordinateur spécial. J'ai utilisé mon ordinateur personnel et Internet. N'importe qui au monde pourrait faire ce que je fais en ce moment. N'importe qui peut visiter un site web pourvu qu'il ait un ordinateur, un navigateur et accès à Internet.

Voici ce que j'ai vu dans mon navigateur lorsque j'ai visité le site web du Sénat du Canada. Ce n'est que la première page. La première chose que vous voyez est cette image de l'édifice du Centre. Je veux parler de cette image. Au lieu d'être une jolie photographie, supposons que ce soit quelque chose de très inquiétant.

Comment suis-je arrivé à cette page? Vous verrez en haut de la page quelque chose que l'on appelle une adresse URL. Je l'ai entourée ici. C'est l'adresse. C'est l'emplacement de cette page sur Internet. Je m'y suis rendu comme le font la plupart des gens. J'ai

words “Senate” and “Canada,” and it turns out this is the number one choice. The point is that my browser needed to have this information to go to the website in the first place. There would not have been a connection otherwise.

My home computer starts with this information. You can see at the top of the page that it says “sen.parl.gc.ca.” That is the address on the Internet of this website. My point is that that is actually what I start with, the URL, the uniform resource locator. I got it because I got the image that was on the web page. This piece of information actually comes first. That is one of the pieces of information that this bill talks about. Here I am just an ordinary user. Not only do I have the image, but I already have that piece of information. I would not have got it if I did not have it. That is just the way browsers work. They need to have an address.

It is like saying if I want to telephone someone, I suppose I would have to know their telephone number, would I not? If I did not know it, I would look it up and call them; so my browser had that information.

This is just the appearance that most people see in the browser, but if you dig deeper, it turns out my home computer got more information just because I looked at this Senate of Canada web page.

The next page is called the source of the page. My browser got instructions from the Senate’s web server about what to do. It said here is my web page; here is some text and it should look like this. Here is an image, go get it. These are the actual instructions. Anyone can see what they are. They are not a secret.

I opened my browser and said view the source; show me the instructions that you just got from the web server to do that web page and here they are. Look at the information that is there.

The second point is the key one. Somewhere there is the name of the file that has that picture. I circled that right in the middle. That is another thing I know right away just because I got it. I had to look up the name. It was not sitting there on the main page, but my browser had that information; I have it.

You see, I know it is called images/banner-b.jpg; that is the name of a file that holds that image. I know that must be the name on the Senate web server, which I already know has the name sen.parl.gc.ca, so I knew that.

The bill also talks about an Internet protocol address. What is that? It is just a number. You see that name at the beginning, sen.parl.gc.ca. We are human beings; we like names; we remember them. We are not very good at numbers, but computers, believe me, are good at numbers. In fact, they only work with numbers, so that name is always translated to a number.

utilisé un moteur de recherche comme Google. J’ai écrit les mots « Sénat » et « Canada » et il se trouve que c’est le premier choix. Le fait est que mon navigateur avait besoin de cette information pour se rendre sur le site web. Il n’aurait pas été possible d’établir une connexion autrement.

Mon ordinateur personnel commence avec cette information. Vous pouvez lire en haut de la page « sen.parl.gc.ca. ». C’est l’adresse de ce site web sur Internet. C’est donc avec cela que je commence, l’URL, le localisateur de ressources uniformes. Je l’ai obtenu parce que je suis arrivé sur l’image qui se trouvait sur la page web. En fait, cette information vient normalement en premier. C’est un des éléments d’information dont parle le projet de loi. Je ne suis qu’un simple utilisateur. J’ai non seulement eu accès à cette image, mais j’ai aussi obtenu cet élément d’information. Je n’aurais pas pu avoir l’un sans l’autre. C’est la façon dont fonctionnent les navigateurs. Ils ont besoin d’une adresse.

C’est comme pour téléphoner. Si je veux appeler quelqu’un par téléphone, je dois connaître son numéro, n’est-ce pas? Si je ne le connais pas, il faut que je le cherche et je peux ensuite le composer; mon navigateur avait donc cette information.

C’est simplement ce qui voient la plupart des gens qui utilisent un navigateur, mais si vous allez plus loin, vous constaterez que mon ordinateur personnel peut obtenir d’autre information du seul fait que j’ai affiché la page web du Sénat du Canada.

La page suivante est ce qu’on appelle la source de la page. Mon navigateur a reçu de la part du serveur web du Sénat des directives au sujet de ce qu’il doit faire. La directive dit voici ma page web; voici du texte et il devrait ressembler à ceci. Voici une image, va la chercher. Ce sont les directives qui sont réellement données. Tout le monde peut les voir. Elles ne sont pas secrètes.

J’ai ouvert mon navigateur et je lui ai dit de regarder la source, de me montrer les directives qu’il vient de recevoir du serveur web pour montrer cette page web et les voici. Regardez l’information qui se trouve là.

Le deuxième point est le point essentiel. Le nom du fichier où se trouve cette image existe quelque part. Je l’ai encerclé au milieu de la page. C’est une autre chose que je connais immédiatement, pour la simple raison que je l’ai obtenu. Il a fallu que je cherche le nom. Cela ne se trouvait pas sur la page principale, mais mon navigateur avait cette information. Je l’ai aussi.

Vous voyez, je sais que cela s’appelle images/banner-b.jpg; c’est le nom du fichier qui contient cette image. Je sais que cela doit être le nom qu’il porte sur le serveur web du Sénat, dont je connais déjà le nom, sen.parl.gc.ca, de sorte que j’ai appris cela.

Le projet de loi parle également d’adresse de protocole Internet. Qu’est-ce que c’est? C’est un simple nombre. Vous voyez ce nom au début, sen.parl.gc.ca. Nous sommes des êtres humains; nous aimons les noms; nous nous en souvenons. Nous ne sommes pas très bons avec les chiffres, mais les ordinateurs, je peux vous le dire, s’y connaissent très bien en chiffres. En fait, ils fonctionnent uniquement avec des chiffres, de sorte que ce nom est toujours transformé en une série de chiffres.

Again, on my home computer, I said I wonder what that number is. I looked it up. There are also websites that can do this. It is easy. It is free information.

You can think of it almost like the phone book. I do not know someone's phone number but I look it up. A lot of people these days use 411 websites to look up people's phone numbers. Anyone in the world can look up what the Internet protocol address is of any server. It is even better than the phone companies. There is no such thing as an unlisted number; everything that has a name has a number and you can look it up.

I decided to say, I wonder what the number is for `sen.parl.gc.ca`. You can see the answer is in the middle. The other information is not important, but there is the key bit; it turns out it has that number. That number is unique in the world. No other Internet-connected computer has that particular number, except the Senate web server.

The next one is not so important, but it turns out the Internet is all about communicating information between computers. The way the information appears when it goes over wires or wireless networks is called "packets." The whole thing is not sent at once. It is sent in small pieces, but every one of these pieces has complete information.

I think in my brief I used the analogy of a postcard. Postcards are small, but if they get to where they are going they must have had the final address correct. You have your picture and your address.

The Internet has even more information. I just picked out a few of the interesting pieces from one little packet. These things go around thousands per second — this is just one. I thought, look at that, there is that IP address again, so I know who was talking to me at the time. That is the IP address of the Senate website. I happened to say this is the part where I ask for that image. There is the name of the image from the web server.

The final part is the key part and it relates to the bill talking about advising an Internet service provider. I just went to the Senate website and I said, there is a nice picture of the Centre Block. I want to compliment someone on it, as opposed to reporting offensive child pornography. It turns out you can also freely and easily and publicly find out who controls the network. This is also available.

I used a command; I could have used websites to do this. I already know the IP address. All I did was look up from the name — and that came from my web browser — so I can look up who is responsible for the network. Every network has a name.

Encore une fois, sur mon ordinateur personnel, j'ai dit que je me demandais quel était ce nombre. Je l'ai cherché. Il y a aussi des sites web qui peuvent le faire. C'est facile. C'est de l'information gratuite.

Vous pourrez presque comparer cela à un annuaire téléphonique. Je ne connais pas le numéro de téléphone de quelqu'un, mais je peux le trouver. De nos jours, il y a beaucoup de gens qui utilisent le site web 411 pour trouver un numéro de téléphone. N'importe qui dans le monde entier peut chercher l'adresse de protocole Internet de n'importe quel serveur. C'est même plus facile que pour le téléphone. Il n'y a pas de numéros confidentiels; tout ce qui a un nom est associé à une série de chiffres, et il est possible de les trouver.

Je me suis dit, je me demande quel est le nombre qui correspond à `sen.parl.gc.ca`. Vous pouvez voir que la réponse se trouve au milieu. Les autres renseignements ne sont pas importants, mais voici l'élément clé; il se trouve qu'il porte ce nombre. Ce nombre est unique au monde. Il n'y a aucun ordinateur relié à Internet qui possède ce nombre particulier, à l'exception du serveur web du Sénat.

L'élément suivant n'est pas très important, mais il faut savoir qu'Internet sert principalement à transmettre de l'information d'un ordinateur à un autre. L'information est transmise par des réseaux filaires ou non filaires sous la forme de « paquets ». Toute l'information n'est pas envoyée d'un seul coup. Elle est débitée en petits morceaux et chacun de ces petits morceaux contient des renseignements complets.

Je pense que dans ma mémoire, j'ai fait une comparaison avec une carte postale. Les cartes postales sont petites mais si on veut qu'elles arrivent à leur destination, il faut que l'adresse finale soit exacte. Vous avez votre image et votre adresse.

Internet recèle encore plus de renseignements que cela. Je n'ai fait que prélever dans un petit paquet de données, quelques éléments intéressants. Il y en a des milliers par seconde — ce n'en est qu'un exemple. Je me suis dit, tiens, encore cette adresse Internet. Je savais donc avec qui j'avais été en communication. C'est l'adresse Internet du site web du Sénat. Et c'est à ce moment-là que je demande l'image. Et voilà le nom de l'image telle qu'elle provient du serveur.

La dernière partie est la partie clé. Elle concerne la disposition du projet de loi où l'on parle d'un fournisseur de services Internet qui est avisé d'une adresse. J'ai simplement consulté le site Internet du Sénat, et j'y ai trouvé cette photo de l'édifice du Centre. Il conviendrait, en l'occurrence, de féliciter le photographe et non de signaler la présence de pornographie juvénile. On constate donc que l'on peut librement, facilement et publiquement savoir qui contrôle le réseau. Ce renseignement, lui aussi, disponible.

J'ai simplement appuyé sur une commande; j'aurais pu aussi utiliser pour cela des sites Internet. À partir du moment où je connais l'adresse Internet. Je n'ai qu'à rechercher le nom — que j'ai pu trouver au moyen de mon navigateur — et cela me permet de connaître le nom du responsable du réseau. Tous les réseaux ont en effet un nom.

The second part talks more about the details. What are the details about this particular network? You can see there is technical information like the actual number identity of the network, but you look further and there is an address. There is a responsible person. There is a telephone number; there are even web links for contacts and so on. This is the kind of information that could be used for advising an ISP about it.

My point is that the bill talks about “advising an ISP.” How do you know who the ISP is? The Internet is a very big place and it changes very quickly. There are millions of networks in the world. There are probably several hundred thousand Internet service providers.

Which one do you notify? I just showed you; it follows. There is the content, the picture — how did you get it? There is an address. The address can be translated to an Internet protocol address. From the Internet protocol address, you can always figure out the network because the information is right there; and when you know the network, there is always someone responsible.

If you cannot get them, everyone is connected to everyone else — someone bigger than someone else. For example, since I looked it up, the Senate web server is in a network that is part of a much larger network that, at least in Ottawa, is controlled by Bell Canada. Everyone gets connections to networks other than their own through someone else.

My point in these opening remarks was basically how open the Internet is. This information was all there right in front of me. When I got the content — let us say we are talking now about offensive and criminal child pornography — I got all this information as well. Therefore, the issue is then about reporting.

With this information, I not only have data but I have metadata — in other words, the actual content and the description about the content. Bill C-22 talks about how it should be ISPs giving the information about two specific pieces of metadata, IP addresses and URLs, to competent authorities. My point is — is that really necessary?

Anyone capable of advising an ISP knows who the ISP is. Of course they do, because they have the IP and the URL. I would think that someone with evidence of crime should report crime; and that the more direct — this is up to you to decide — the better. This is the evidence; why am I not reporting this information?

La deuxième partie entre davantage dans le détail. Quels détails peut-on obtenir sur ce réseau? Vous apercevez un certain nombre de détails techniques, tels que le numéro d'identité du réseau, mais si vous continuez à chercher, vous trouvez l'adresse. Cette adresse est celle du responsable. Il y a un numéro de téléphone, et même des liens Internet permettant d'entrer en contact. Voilà le genre d'indications qui peuvent être transmises à un fournisseur de services Internet pour lui signaler la présence de pornographie juvénile.

Or, aux termes du projet de loi, on doit aviser le fournisseur de services Internet. Mais, comment savoir qui il est? Internet est un vaste espace en constante évolution. Il y a dans le monde des millions de réseaux. Il existe sans doute plusieurs centaines de milliers de fournisseurs de services Internet.

Quel est celui qu'il convient d'aviser? Cela, je viens de l'expliquer. Il y a le contenu, la photo — comment l'avez-vous obtenue? Eh bien, il y a une adresse. Cette adresse permet de connaître l'adresse de protocole Internet. À partir de l'adresse de protocole Internet, vous pouvez trouver le réseau, car vous avez sous les yeux tous les renseignements nécessaires. Or, à partir du moment où vous connaissez l'identité du réseau, vous pouvez remonter jusqu'au responsable.

Si vous n'y parvenez pas, souvenez-vous que tout le monde est interconnecté — il y a des maillons plus importants que d'autres. Je constate ainsi, car c'est à lui que je me suis intéressé, que le serveur web du Sénat fait partie d'un réseau qui fait lui-même partie d'un réseau beaucoup plus étendu qui est, du moins à Ottawa, contrôlé par Bell Canada. Chacun passe par quelqu'un d'autre pour se connecter à un réseau.

S'il y a une idée que je souhaite faire passer ce soir, c'est qu'Internet est un espace ouvert. Les renseignements que je cherchais étaient là, facilement accessibles. Lorsque, donc, je suis parvenu au contenu — disons qu'il s'agisse de pornographie juvénile —, j'ai pu, en même temps, obtenir tous ces renseignements. La question qui se pose est donc effectivement celle de la déclaration.

Les renseignements en question comprennent non seulement des données, mais des métadonnées — autrement dit, le contenu en question ainsi qu'une description de celui-ci. Selon le projet de loi C-22, c'est aux FSI qu'il appartiendra de fournir aux autorités compétentes deux éléments précis de métadonnées, l'adresse Internet et le localisateur URL. Mais je me demande si cela est nécessaire?

Ceux qui sont en mesure d'aviser un FSI, savent bien de qui il s'agit. C'est évident, étant donné qu'ils possèdent l'adresse Internet et le localisateur URL. Selon moi, toute personne au courant d'un acte criminel devrait le signaler, et plus elle est à même de le faire directement — et là c'est à vous d'en décider — mieux c'est. Dans la mesure où j'ai des indices d'un acte criminel, pourquoi ne les porterais-je pas à l'attention des autorités?

There is much more to it, but I would welcome any of your remarks upon this or my brief — just how the bill works, or about IPs or URLs or anything else.

Senator Wallace: It is hard to know where to start.

Senator Angus: Start with the URL.

Senator Wallace: I will leave that to you. I found it easier when you were using the analogy of the phone book. I can relate to that; it is just numbers in the book and you have the book. That was useful to understand how all of this connects together, but I am having trouble with what your conclusion seems to be.

The purpose of the bill is to increase the opportunities for authorities to close down these child pornography websites. They have to be aware of them in order to be able to take action against them; and the timeliness with which they do take that action is obviously critical for the victims who are the subject of the child pornography. It is the time limits and being able to react to it, which comes back to being aware of its existence.

I was taking from your comments that all of this information is somehow out there in cyberspace and perhaps the police could spend their time going through cyberspace trying to find it. Your words were that someone who witnesses crime should report it. Well, if an ISP sees something that could constitute pornographic material on the Internet, what possible problem could there be in having them bring that to the attention of the authorities? Do the victims not benefit from that?

Mr. MacKay: The bill talks about advising ISPs, so the starting point of Bill C-22 starts with advice. If it just started with ISPs detecting child pornography on their own network, that would be fine, but the starting point is upon being advised.

Senator Wallace: If you are talking about clause 2 of the bill, it is not the ISP that somehow is to be advised. If any person becomes aware of the existence of this material in the course of an ISP carrying on its business or otherwise, then they have the obligation to report.

Mr. MacKay: Right.

Senator Wallace: My sense is you feel that this places an undue requirement on an ISP and their only responsibility should be to look after their own system. In the course of their business, if they find something else out there, that is someone else's problem. I hope that is not your conclusion, but I am taking that from your comments.

Mr. MacKay: No, not at all. My understanding, and the way I read the bill, is it starts with someone advising an ISP about an incidence of child pornography on their network. It then introduces an obligation on the ISP to report two pieces of

On pourrait en dire beaucoup plus, mais j'aimerais bien savoir ce que vous pensez de ce que j'avance dans mon mémoire — sur le fonctionnement éventuel des dispositions du projet de loi, ou sur les adresses Internet ou les localisateurs URL, par exemple.

Le sénateur Wallace : On ne sait pas trop par où commencer.

Le sénateur Angus : Commençons par le localisateur URL.

Le sénateur Wallace : Je vous laisse le soin de traiter de ce sujet. Je m'y retrouvais un peu mieux lorsque vous citiez l'exemple du bottin de téléphone. Je trouvais cela plus parlant. Il y a l'annuaire et puis il y a les numéros qui y sont inscrits. Je voyais mieux comment tout cela s'imbrique, mais je vous suis moins au niveau de vos conclusions.

Ce projet de loi doit donner aux autorités de nouveaux moyens de fermer les sites Internet de pornographie juvénile. Or, pour tous les fermer, les autorités doivent pouvoir les repérer, et la rapidité de leur intervention revêt manifestement une importance essentielle pour les jeunes victimes. Il s'agit d'agir et d'agir vite, mais, pour cela, il faut pouvoir repérer les sites en question.

J'ai cru comprendre de ce que vous nous avez dit, que toutes les indications voulues se trouvent là, à l'état libre, dans le cyberspace et que la police pourrait, si l'on peut dire, patrouiller ce cyberspace et y recueillir les renseignements nécessaires. Vous avez-vous-même dit que celui qui constate un acte criminel devrait le signaler aux autorités. Eh bien, si un FSI repère, sur Internet, de la pornographie juvénile, pourquoi ne pas l'obliger à porter cela à l'attention des autorités? Ne pensez-vous pas que les victimes seraient les premiers bénéficiaires d'une telle mesure?

M. MacKay : Le projet de loi parle d'aviser les FSI, et le point de départ de ces dispositions c'est donc cet avis donné à un FSI. Si le projet de loi imposait une telle déclaration à tout FSI constatant de la pornographie juvénile sur son réseau, je n'y verrais aucun inconvénient, mais en l'occurrence, tout ne commence que lorsque le FSI est avisé.

Le sénateur Wallace : Si vous entendez par cela l'article 2 du projet de loi, je précise que ce n'est pas le FSI qui doit être avisé. Toute personne qui constate l'existence de pornographie juvénile dans le cadre des services offerts par un FSI est tenue de le signaler.

M. MacKay : Bon.

Le sénateur Wallace : J'ai l'impression que, d'après vous, cela impose aux FSI, une obligation démesurée, car leur unique responsabilité devrait consister à s'occuper de leur propre système. Si, dans le cadre de leur entreprise, ils constatent l'existence de quelque chose de répréhensible, ce n'est pas vraiment leur problème. J'espère que ce n'est pas ce que vous entendez, mais c'est l'impression que j'ai retirée de vos propos.

M. MacKay : Non, pas du tout. Si j'ai bien compris le mécanisme envisagé, il y a, au départ, quelqu'un qui avise un FSI que de la pornographie juvénile se trouve sur son réseau. C'est cela qui déclenche, pour le FSI, l'obligation de fournir aux

metadata, an IP and a URL, to competent authorities. My point is simply a logical one. How did someone know which of all the ISPs in the world to advise? The answer? They already have those two pieces of metadata right in front of them. Otherwise, they would not know. IP addresses do not just identify hosts on networks. They identify the networks themselves, hence the ISPs. My point is that, if we want to be more quick about this, more reactive, more responsive, why introduce this roundabout procedure? Why does the advice not go straight to competent authorities? Why is there not an obligation on witnesses to crime to report crime?

Senator Wallace: I will take one more crack at it. On that point, I think you are referring to clause 2, which indicates that if a person is advised in the course of providing an Internet service of the address, then it must be reported. The person could be an individual or a corporation. If the provider, the ISP, the corporation, is advised of such an address, the obligation would be on the corporation. A person is also an individual. It could be an individual employee working for an ISP. It would seem to me that clause 2 would capture them. That individual would have the obligation. It is in the business. It is working for a provider of Internet service. The individual would have the obligation to report. Once again, what is the conundrum with that?

Mr. MacKay: We have the case of someone saying, “I saw offensive content on your website.”

Senator Wallace: On a website. Not ours, but a website.

Mr. MacKay: It is a website that appears to be under your control. Do we want third-party witnesses? Do we want people to talk about other people’s networks?

Senator Wallace: The person that finds it would not be reporting it to the potential offending —

Mr. MacKay: They might be, under this bill. How do we know the ISP is not the criminal organization?

Senator Wallace: I do not intend to get into a debate with you. I apologize for that. My understanding of clause 2 is that the only obligation on the person who has come upon this potentially offending third-party Internet service provider would be then to report it to an organization.

Mr. MacKay: They would say, “Someone said there is offensive content on a network, and we are passing along the IP of this network. It is true that that IP is in this network, as anyone in the world could have told you.”

The Chair: Might I have a little supplementary?

autorités compétentes deux éléments de métadonnées, l’adresse Internet et le localisateur URL. Je me place entièrement du point de vue de la logique. Comment la personne en question va-t-elle savoir, de tous les FSI qui existent dans le monde, celui qu’il convient d’aviser? Quelle est la réponse à cette question. Cette personne hypothétique dispose de deux éléments de métadonnées, sans quoi elle ne saurait pas. L’adresse Internet n’identifie pas simplement le serveur hôte, mais le réseau, et donc le FSI. Ce que je veux dire c’est que dans la mesure où nous souhaitons pouvoir réagir plus rapidement, pourquoi prévoir une procédure aussi indirecte que celle-ci? Pourquoi ne pas faire aviser directement les autorités compétentes? Pourquoi ne pas prévoir que toute personne qui constate une activité criminelle doit la signaler?

Le sénateur Wallace : Je reprends mon raisonnement. Je crois qu’en disant cela vous parlez de l’article 2, selon lequel toute personne qui est ainsi avisée dans le cadre des services Internet qu’elle fournit au public, doit le signaler. Ce peut être un individu ou une entreprise. Si le fournisseur de services Internet, l’entreprise donc, est avisée d’une telle adresse, c’est à elle qu’incombe l’obligation. Il pourrait également s’agir d’un individu. À supposer que ce soit un employé, par exemple, d’un FSI. Les deux cas de figure sont englobés par l’article 2. En l’occurrence, ce serait à l’individu de signaler la chose. Cela se situe dans le cadre du service Internet qu’il fournit dans la mesure où l’intéressé est employé par un fournisseur de services Internet. Cet individu serait effectivement tenu de communiquer le renseignement. Je ne vois pas, encore une fois, en quoi cela pose un problème?

M. MacKay : La personne va donc aller dire « J’ai constaté, sur votre site Internet, un contenu abominable. »

Le sénateur Wallace : Oui, sur un site Internet. Pas nécessairement sur le nôtre, sur n’importe quel site Internet.

M. MacKay : Sur un site Internet qui semble relever de votre contrôle. Allons-nous faire appel à des témoins tiers? Souhaitons-nous encourager les gens à dénoncer les réseaux d’autrui?

Le sénateur Wallace : Mais la personne en question ne doit pas communiquer ce renseignement à l’auteur éventuel de l’infraction...

M. MacKay : Aux termes du projet de loi, cela pourrait cependant arriver. Comment savoir si le FSI en question n’est pas, justement, l’organisation criminelle responsable du contenu que l’on cherche à réprimer?

Le sénateur Wallace : Je ne veux pas épiloguer sur la question. Vous m’excuserez. D’après moi, l’article 2 crée uniquement, pour la personne qui tombe sur un FSI tiers qui est peut-être en infraction, l’obligation de le signaler à une organisation.

M. MacKay : Il s’agit simplement pour eux alors de dire, « Quelqu’un a constaté, sur un réseau, un contenu prohibé et nous vous signalons le FSI de ce réseau. Le FSI en question fait effectivement partie de ce réseau, comme chacun aurait pu vous le dire ».

La présidente : Me permettez-vous une rapide question complémentaire?

Senator Wallace: Yes, indeed.

The Chair: I would take issue with your “as anyone in the world could have told you.” As anyone in the world who is as technologically literate as you — but the people around this table, honourable senators all, are also part of anyone in the world, and I would bet you my right arm that not one of us would have known how to notify anyone about all the information that you have now explained to us is available, just by dint of having that URL up on their screen.

Mr. MacKay: That is true, but the bill presupposes someone who is capable of advising.

The Chair: That is my question. Correct me if I am wrong, Mr. MacKay, but you seem to me to be saying that there is no point in having me turn to someone who knows more about this technology than I do, if I stumble upon what looks to me like a site devoted to child pornography. I am not sure what you are saying.

Senator Angus: That is right.

The Chair: Somewhere in there, I got lost. Senator Wallace, you can help me here.

Senator Wallace: At least I am not alone in this. I know I am in good company. This is probably an oversimplification. I take from what you are saying that, somewhere in this phone book is an offender, and I know which phone number it is and I know the address, but I will not tell you because you have a phone book as well.

Mr. MacKay: I am trying to follow your analogy there.

The Chair: Ratchet it down to words with one syllable for us, and for many other people in the world.

Senator Angus: They may be watching us on the webcast, for example.

The Chair: Let Mr. MacKay take a shot at answering this, and then Senator Watt can have a quick supplementary. We will be well into overtime.

Mr. MacKay: It is absolutely correct that most people not only do not know about IP addresses, but they do not even know about URLs, because they click on links and just follow them, and the content just appears in front of them. They see it and are upset by it. They do not know who to talk to. If they talk to anyone, they probably talk to their own ISP, because they are not doing this lookup of whatever it is. Their own ISP probably has absolutely nothing to do with it.

Le sénateur Wallace : Oui, bien sûr.

La présidente : Je ne comprends pas que vous ajoutiez « Comme chacun aurait pu vous le dire ». Peut-être comme aurait pu vous le dire toute personne ayant, comme vous, des connaissances technologiques de pointe — mais ceux et celles qui sont assis autour de cette table, tous des honorables sénateurs, font, eux aussi, partie de tout le monde et je suis persuadée qu’il n’y en a pas un entre nous qui aurait su comment communiquer les renseignements utiles comme vous venez de nous l’expliquer à partir du localisateur URL qui se trouve sur leur écran.

M. MacKay : C’est vrai, mais le projet de loi s’adresse tout de même à des gens qui seraient, eux, en mesure d’aviser le fournisseur de services Internet?

La présidente : C’est justement ma question. Dites-moi, M. MacKay, si j’ai mal compris. Ne dites-vous pas que si je tombe sur un site qui me semble abriter de la pornographie juvénile, je ne vois pas pourquoi j’en ferais part à quelqu’un qui possède, en matière de technologie, des connaissances plus poussées que moi. Je ne comprends pas très bien où vous voulez en venir.

Le sénateur Angus : En effet.

La présidente : Je ne m’y retrouve plus très bien. Sénateur Wallace, j’ai besoin de votre aide.

Le sénateur Wallace : Je vois que je ne suis pas le seul. Je me retrouve en bonne compagnie. Je sais qu’en disant cela je simplifie à outrance. Mais si j’ai bien compris, selon vous, il y a, disons dans l’annuaire de téléphone, un contrevenant dont je connais le numéro de téléphone et l’adresse, mais je ne vous les communiquerai pas puisque vous disposez, vous aussi, de cet annuaire de téléphone.

M. MacKay : J’essaie de saisir le sens de votre exemple.

La présidente : Je vous demande de bien vouloir expliquer cela en termes simples, à la fois pour nous et pour tous les autres qui pourraient avoir un peu de mal à suivre.

Le sénateur Angus : Dont certains qui suivent peut-être la séance diffusée en direct sur le web.

La présidente : Laissons à M. MacKay le soin de répondre, et puis le sénateur Watt pourra poser très rapidement une question complémentaire. Nous aurons largement dépassé notre horaire.

M. MacKay : Il est vrai que la plupart des gens non seulement ne savent pas ce qu’est une adresse Internet, mais ne savent même pas ce qu’est un localisateur URL, puisqu’ils ne font que cliquer sur le lien pour voir apparaître devant eux le contenu. Il peut arriver qu’ils en soient bouleversés, sans savoir pourtant à qui signaler cela. S’ils le signalent à quelqu’un, ce sera probablement à leur FSI, étant donné qu’ils ne vont pas vérifier la source. Or, il est vraisemblable que leur FSI n’a absolument rien à voir avec le contenu en question.

As I said, the information is there and the police, for example, or other competent authorities could also look it up. Is there a benefit to have a special onus on an ISP to handle just that particular, to be a relay for that IP information? I just do not know. It seems to me that it is a roundabout way of reporting crime.

Senator Wallace: Thank you.

The Chair: I will restrain myself. I told Senator Watt he could have a supplementary.

Senator Watt: I might be able to provide a little bit of help here, if I understand what has been dealt with up until now.

I am not specialized. I have no knowledge whatsoever in terms of what you are saying, but I am going by what I heard. You are basically talking about what people are doing with information that is already available. Anyone can access that information that you highlighted and walked us through in terms of the information and how can you get the information.

Internet service providers also have that information, and you have that information. All you have to do is look it up. I think you are telling us: Why make it complicated when it is a straightforward issue? All you have to do is report it because the information is already there. That is what I am hearing from our witnesses.

Mr. MacKay: I made a point in my brief that a distinction people commonly make is that Internet service providers are some big company and that we are just home users and we are not the same. I have been working with the Internet for 20 years and I know that it is much more of an equal partnership; it is much more like a conversation. This is not a technology like television, which you watch. This is not a technology like radio, where you listen. It is much more like a conversation. At any time the roles could be reversed.

Could an ISP have this information? Of course. In fact it is their job to manage it every day, right? I teach my customers how to build the DNS servers, domain name servers, that can do that telephone book. I know how to build a telephone book on the Internet and can I teach other system administrators how to do it.

Only a tiny number of people need to know how to do that. As far as the rest of us are concerned, the mapping between someone's name and a number can be magic as long as it works. The ISP knows how to do that.

However, home computers, PDAs, personal digital assistants, and so on are extremely powerful and the information could all be there. Your home computer could become a web server at the flip of a switch. It is true that only a small number of people have the

J'insiste bien, donc, sur le fait que les indicateurs sont là et que la police notamment, ou d'autres autorités compétentes, sont parfaitement en mesure de les trouver. Quel est l'intérêt d'obliger les FSI en particulier à servir de relais à ces indications concernant le protocole Internet en question? Je ne sais pas. C'est, d'après moi, une manière un peu détournée de signaler un acte criminel.

Le sénateur Wallace : Je vous remercie.

La présidente : Je vais m'abstenir. J'ai effectivement dit au sénateur Watt qu'il pourrait poser une question complémentaire.

Le sénateur Watt : Peut-être vais-je pouvoir éclaircir un petit peu le débat, dans la mesure, bien sûr, où je comprends de quoi il s'agit.

Je ne suis pas spécialiste de ce domaine. Je n'ai aucune connaissance des choses que vous venez de nous expliquer et je dois par conséquent m'en tenir à ce que je vous ai entendu dire. Vous posez en fait la question de savoir quoi faire de ces indications auxquelles chacun peut avoir facilement accès. Chacun, en effet, peut trouver les renseignements en question en suivant la démarche que vous nous avez expliquée.

Les fournisseurs de services Internet ont, comme vous et moi, accès à ces renseignements. Il suffit de les chercher. Vous estimez donc qu'il n'y a pas lieu de compliquer quelque chose de parfaitement simple. Il s'agit seulement de communiquer les renseignements qui se trouvent là. C'est ce qu'affirment nos témoins.

M. MacKay : J'ai, dans mon exposé, insisté sur le fait que les gens pensent généralement que les fournisseurs de services Internet sont de grosses entreprises, les opposant ainsi aux simples utilisateurs et faisant entre les deux une grande distinction. Or, cela fait 20 ans que je m'occupe d'Internet, et je sais que la situation respective des FSI et des utilisateurs est beaucoup plus égale qu'on ne le pense en général. C'est plutôt comme une conversation. Ce n'est pas un moyen de diffusion que l'on regarde, comme la télévision. Ce n'est pas non plus comme la radio, que l'on écoute, c'est beaucoup plus comme une conversation et, à tout moment, les rôles peuvent s'inverser.

Un FSI peut-il obtenir les indications en question? Bien sûr. Cela fait d'ailleurs partie de son travail. J'enseigne à ma clientèle comment créer des serveurs DNS, des serveurs de nom de domaine, c'est-à-dire, pour reprendre l'analogie de tout à l'heure, comment compiler un annuaire de téléphone. Je sais comment procéder, et j'enseigne cela à d'autres gestionnaires de systèmes.

Seul un tout petit nombre de personnes ont besoin de savoir comment faire cela. Pour les autres, la cartographie des noms et des numéros de domaine peut paraître un sujet hermétique; il leur suffit que cela fonctionne correctement. Or, les FSI, eux, savent comment s'y prendre.

Les ordinateurs personnels ou les ANP, c'est-à-dire les assistants numériques, sont des appareils extrêmement puissants qui donnent accès, notamment, aux renseignements dont nous venons de parler. Une simple opération permet de transformer

technological knowledge to do it, but that number is growing and growing, especially as it is made easier with, for example, social networking websites and so on.

The idea of the distinction between an ISP, which is a company that provides a service that is completely separate from their customers, who are recipients of service, is not so ironclad. It is much more of a peer type of network, and it has always been that way. It has always been that the information is everywhere and they are equal partners.

[Translation]

Senator Carignan: I am trying to understand your point of view. I believe you have to read the bill very carefully. The problem may stem from your comment on the text of the bill. I do not know whether you have it before you, but clause 3 reads as follows:

If a person is advised, in the course of providing an Internet service to the public — that is, the Internet service provider — of an Internet Protocol Address or a Uniform Resource Locator where child pornography may be available to the public, the person must report that address as soon as feasible.

So I am a customer, and I do not know a lot about computers, but enough to know how to find an Internet address, as you showed us earlier, and I call up my provider. It receives a very large number of calls every week and cannot do all the work; that is why it helps an agency called the Canadian Centre for Child Protection, whose representatives appeared before you earlier. It helps that centre do the sorting, or else it will have to hire full-time staff to perform that task. It prefers to help a third agency to do that work.

The bill therefore frames a practice that has already developed in the industry. As the privacy commissioner said earlier, it makes no sense for a practice of preserving private information, as sensitive as this information is, not to be supported by a legislative framework, and clause 3 therefore addresses this difficulty that Internet services providers have responding to all complaints or requests that may come from their customers.

This is forwarded to the agency that the government will designate by regulation, which should be Cybertip.ca.

Clause 4:

If a person who provides an Internet service to the public has reasonable grounds to believe that their Internet service is being or has been used to commit a child pornography offence. . .

votre ordinateur personnel en serveur web. Il est vrai que seul un petit nombre de personnes possèdent les connaissances techniques qui permettent de faire cela, mais leur nombre va croissant et cela devient d'ailleurs de plus en plus facile en raison notamment des sites de réseautage social.

Ainsi, la distinction qui est faite généralement entre un FSI, c'est-à-dire l'entreprise qui fournit un service, et ses clients, c'est-à-dire ceux auxquels ce service est fourni, n'a rien d'absolu. Il s'agit davantage d'une relation entre égaux et cela a d'ailleurs toujours été vrai. Il a toujours été vrai que l'information est à la portée de tous et qu'il s'agit plutôt d'une relation d'égalité entre partenaires.

[Français]

Le sénateur Carignan : J'essaie de comprendre votre point de vue. Je pense qu'il faut lire le projet de loi de façon précise. La problématique origine peut-être de votre commentaire par rapport au texte du projet de loi. Je ne sais pas si vous l'avez devant vous, mais l'article 3 dit ceci :

La personne qui est avisée, dans le cadre des services Internet qu'elle fournit au public — donc, le fournisseur des services Internet —, d'une adresse de protocole Internet ou d'une adresse URL où pourrait se trouver de la pornographie juvénile accessible au public communique l'adresse dans les meilleurs délais.

Donc, je suis client, je n'ai pas de grandes connaissances en informatique, mais suffisamment pour savoir repérer l'adresse Internet, comme vous nous l'avez montré tout à l'heure, et j'appelle mon fournisseur. Celui-ci reçoit des appels en quantité industrielle, à toutes les semaines, et ne peut pas faire tout ce travail; c'est pour cela qu'il aide un organisme qui s'appelle le Centre canadien de protection de l'enfance, dont les représentants ont comparu devant nous tout à l'heure. Il aide ce centre pour qu'il fasse le tri, sinon il devra se doter de personnel à temps plein pour effectuer cette tâche. Il préfère aider un organisme tiers pour que ce travail soit accompli.

Le projet de loi encadre donc une pratique qui s'est déjà développée dans l'industrie. La commissaire à la protection de la vie privée le disait tout à l'heure, cela n'a pas de bon sens qu'une pratique de détention d'informations privées, sensibles comme celles-là, ne soit pas appuyée par un support législatif, et donc, l'article 3 vient palier cette difficulté pour les fournisseurs de services Internet de répondre à toutes ces plaintes ou demandes qui pourraient venir de leurs clients.

C'est transmis à l'organisme que le gouvernement va désigner par règlement, qui devrait être Cyberaide.ca.

L'article 4 :

La personne qui fournit des services Internet au public qui a des motifs raisonnables de croire que ses services Internet sont ou ont été utilisés pour la perpétration d'une infraction relative à la pornographie juvénile [...]

So we are not dealing with the presence or preservation of child pornography; we are dealing with the commission of an offence. The person no longer calls the designated organization; he or she calls the police; he or she has grounds to believe that an offence has been committed and calls the police department responsible for enforcing the law.

I do not understand the issue you submitted to us, that the bill would mean that Internet service providers would conspire.

In my opinion, and you will correct me if I am wrong — here is my question — the Internet service providers have felt a need to act on their own, without there even being a legislative framework for sorting all this information, and we are supporting those service providers by means of a bill; do you not consider that as a help rather than as a charge of conspiracy?

The Chair: Before Mr. MacKay answers, I would point out that, when you cited clauses 3 and 4, I believe they are clauses 2 and 3 in the most recent version of the bill, Senator Carignan.

Senator Carignan: Pardon me; I may have had the wrong version.

[English]

The Chair: That exchange was simply technical references for the record regarding the clauses being quoted. Now let us move to the substance of the question.

Mr. MacKay: I understood the substance of the question to be whether this helps ISPs in their reporting. As far as I know, the substance of the bill is about fines if they do not report this information. In other words, it basically implies that there is a special duty on them to report this crime. However, it does not impose the same requirement upon the original person giving the advice.

I just do not see how that helps an ISP in the job they need to do to regulate their networks in accordance with the law.

[Translation]

Senator Carignan: So your problem is with the fine, not the obligation?

[English]

Mr. MacKay: The obligation is something ISPs will have anyway. I see this opening up a problem for people who are essentially accidental ISPs, or smaller ones. If you have in mind big telcos that have the capability to do extensive logging, to keep large servers with this information and that have the ability to

Donc, on en n'est pas à la présence ou à la conservation de pornographie juvénile, on en est à la perpétration d'une infraction. Elle n'avise plus l'organisme désigné, elle appelle la police; elle a des motifs de croire qu'une infraction a été commise et elle appelle le service de police chargé de l'application de la loi.

Je ne comprends pas la problématique que vous soumettez, à savoir que le projet de loi impliquerait que les fournisseurs de service Internet complotent.

Selon moi, vous me corrigerez si je me trompe — voici ma question —, les fournisseurs de services Internet ont senti le besoin d'agir eux-mêmes, sans même un cadre législatif pour faire le tri de toute cette information, et on vient supporter ces fournisseurs de service à l'aide d'un projet de loi; ne considérez-vous pas cela comme une aide plutôt que comme une accusation de complot?

La présidente : Avant que M. MacKay ne réponde, je signale que quand vous avez cité les articles 3 et 4, je pense que dans la version la plus récente du projet de loi, il s'agit des articles 2 et 3, sénateur Carignan.

Le sénateur Carignan : Je m'excuse, j'ai peut-être la mauvaise version.

[Traduction]

La présidente : Cet échange de propos portait simplement sur des références techniques rappelées aux fins du compte rendu, au sujet des articles du projet de loi qui étaient cités. Passons maintenant au fond même de la question.

M. MacKay : Si j'ai bien compris, il s'agissait de savoir si cela aide effectivement les FSI à faire les déclarations qu'ils seront tenus de faire. Le projet de loi prévoit essentiellement des amendes pour les personnes qui ne communiquent pas les renseignements qu'elles sont tenues de fournir. Cela veut dire qu'on leur impose l'obligation particulière de signaler ce genre d'activité criminelle. Or, cette obligation ne pèse pas sur la personne qui signale initialement l'activité en cause.

Je ne vois pas très bien en quoi cela aide les FSI à faire ce qu'ils doivent faire pour réglementer, conformément aux dispositions applicables, ce qui se passe sur leurs réseaux.

[Français]

Le sénateur Carignan : Donc, votre problème vise l'amende et non pas l'obligation?

[Traduction]

M. MacKay : Cette obligation incombe aux FSI de toute manière. Or, d'après moi, cela risque de créer des problèmes à ceux qui se trouvent presque accidentellement être des FSI, ou des fournisseurs de moindre envergure. Sans doute avez-vous songé aux grosses entreprises de télécommunications qui possèdent les

know about and respond to this, what about smaller ISPs and what about accidental ISPs, which are people who have their machines or networks compromised? They are ISPs.

In a way, I see service providers as secondary victims in this crime, unless they are the originator of it in the first place, which is always a possibility. However, in most cases, they are hosting companies or they are compromised home computers with this information. Any citizen could be the ISP in that case. The bill does not make a distinction in that respect.

Therefore, it opens up a very technical issue about reporting two specific pieces of metadata on anyone who ends up being an Internet service, accidentally or otherwise.

If your question is: Does that help them? I do not know. I think it frightens, or it should frighten, many people who will not understand it or be technically competent if they find themselves in that position.

The Chair: Mr. MacKay, we still have four senators on the list. We are officially in overtime with you, so the question to every senator is: Can you keep your question — singular — tight? Senator Watt, this is an instruction to you too because you are on the list. I am saying that each senator will have one question.

Senator Watt: I have a question.

The Chair: You are on the list. That is why I was harassing you. I will ask Mr. MacKay to keep his answers as tight as he possibly can. The senators on the list are Senators Runciman, Watt, Angus and Boisvenu.

Senator Runciman: An important element of the proposed or old legislation, I will say clause 4, states that, "A person who makes a notification under section 3 must preserve all computer data related to the notification that is in their possession or control for 21 days after the day on which the notification is made." That has real relevance to what we are trying to accomplish in terms of being able to shut down these sites after we discover them and, hopefully, save a child from continued abuse.

I have trouble with what you are saying. We are hearing from the policing community and victims' organizations that this proposed legislation is necessary and that it will be helpful. A report from the National Child Exploitation Coordination Centre tells us about ISPs advertising that they do not cooperate with the police as a way to attract customers. We hear that, in 30 per cent to

moyens d'enregistrer toutes les données qui passent sur leur réseau, d'entretenir de grands serveurs où ces renseignements peuvent être archivés, et qui sont en mesure de suivre tout ce qui se passe, et d'y réagir, mais qu'en est-il des FSI de moindre envergure, ou de personnes qui se trouvent fortuitement être des FSI, des personnes dont les appareils ou les réseaux ont été compromis? Elles sont, pourtant, elles aussi des FSI.

D'après moi, à moins qu'un fournisseur de services ne soit en fait la source des activités criminelles en question, ce qui est toujours possible, les FSI me paraissent plutôt être les victimes subsidiaires de ce genre d'activité. Dans la plupart des cas, il s'agit soit de prestataires de services, soit de personnes dont l'ordinateur personnel a été compromis. Tout citoyen peut ainsi se retrouver FSI. Or, le projet de loi ne fait à cet égard aucune distinction.

Je pose ainsi une question extrêmement technique sur la communication de deux éléments précis de métadonnées au sujet de quelqu'un qui se trouve être un service Internet, peut-être de manière tout à fait fortuite.

Quant à savoir si les dispositions envisagées leur seront utiles, je dois répondre que je ne sais pas. Je crois, cependant, que cela effraie ou devrait effrayer bon nombre de personnes qui n'en comprendront pas la teneur ou qui ne posséderont pas les connaissances techniques nécessaires au cas où ils se retrouveraient dans cette situation.

La présidente : Monsieur MacKay, nous avons encore quatre sénateurs inscrits sur la liste et nous avons officiellement dépassé notre horaire. Je demande par conséquent à chacun de ces sénateurs de s'en tenir à une seule question concise. Sénateur Watt, cette instruction vaut également pour vous puisque vous êtes inscrit sur la liste. Chaque sénateur pourra ainsi poser une question.

Le sénateur Watt : J'aurais une question à poser.

Votre nom figure effectivement sur la liste. C'est d'ailleurs pour cela que je vous ai talonné. Je vais demander à M. MacKay d'être, lui aussi, concis dans ses réponses. Figurent sur la liste les noms des sénateurs Runciman, Watt, Angus et Boisvenu.

Le sénateur Runciman : Selon une disposition importante de l'ancienne version, l'article 4, « La personne qui a donné l'avis prévu à l'article 3 préserve les données informatiques afférentes en sa possession ou à sa disposition pendant 21 jours après la date de l'avis ». J'estime que cela est très important compte tenu de l'objectif visé puisqu'il s'agit de pouvoir fermer les sites que l'on découvre et, espère-t-on, éviter qu'un enfant continue à être maltraité.

Je ne vous suis pas très bien. Des représentants policiers, ainsi que des représentants d'organisations de défense des victimes nous ont affirmé que les dispositions envisagées sont nécessaires et qu'elles seront utiles. Selon un rapport du Centre national de coordination contre l'exploitation des enfants, il y a des FSI qui, dans leur publicité annoncent pour attirer des clients, qu'ils ne

40 per cent of the cases of suspected child abuse on the Internet, the ISP refuses to provide subscriber information. I do not have a question. I disagree with the conclusion you have reached.

The Chair: Do you have a precise answer to the effect that “that is interesting, senator?”

Mr. MacKay: Yes. That is interesting, senator.

Senator Watt: Being a person claiming to understand your presentation, maybe I do understand and maybe I do not. I would like to take it a bit further.

I know for a fact that this is not unregulated in terms of the way the Internet is being used. The CRTC, Canadian Radio-television Telecommunications Commission, is not involved. If they will not come up with a set of regulations for how Internet service providers have to operate in this country or anywhere else, what would you recommend? Would you recommend that they be regulated? That would be another way to ensure that they are honest and do the job they purport to do. You also mentioned a good possibility that some ISPs might act within a communal area.

Mr. MacKay: Absolutely. It is not just one computer. We are talking about the whole network that is a criminal organization.

Senator Watt: Could you tell me what else we need to do? What is your alternative recommendation? You seem to be knocking the bill before us. What alternative do you suggest, if anything at all?

Mr. MacKay: That is a good question. In response, I will say: the alternative that I presented at the conclusion of my longer brief. I talked about something called, a computer emergency response team, CERT. Essentially, it goes back to the past. The Internet, do not forget, started out as essentially a creature of the U.S. government — the military. They called the shots because they controlled the grant money that went to the universities and institutes to develop it. It was cohesive; it had technical rules; and they followed them because if you did not, you were off the network. As it grew, it basically became like the Wild West such that anyone who does the right connection connects in. That does not mean we cannot self regulate. The Internet has these. I talked about requests for comments — the rules that already govern the Internet. They are technical rules. The answer is: Enforce them. We need an active body that works at the Internet at its own level — people who understand this kind of thing. If I just had my finger on the switch of firewall routers, I could stop this in a second. That addresses Senator Runciman’s point about the ISPs pushing back and so on. The answer is in something that reaches them at their own level. The community emergency response team says: Look, you do not want to host this traffic and you do not

collaborent pas avec la police. On nous a dit que dans 30 à 40 p. 100 des cas présumés d’exploitation des enfants sur Internet, le FSI refuse de fournir des renseignements sur les abonnés en cause. Je n’ai aucune question à vous poser. C’est simplement que je ne suis pas d’accord avec la conclusion à laquelle vous êtes parvenu.

La présidente : Souhaitez-vous répondre, ne serait-ce que pour dire qu’il s’agit d’une précision intéressante?

M. MacKay : En effet. Il s’agit là, sénateur, d’une précision intéressante.

Le sénateur Watt : J’estime avoir compris le sens de votre exposé, mais peut-être n’est-ce pas le cas. Je tiens tout de même à ajouter quelque chose.

Je sais pertinemment qu’un tel emploi d’Internet n’est pas actuellement réglementé. Le CRTC, le Conseil canadien de la radiodiffusion et des télécommunications canadiennes n’intervient pas pour l’instant. Que recommandez-vous que l’on fasse dans la mesure où le CRTC ne se décide pas à réglementer l’activité des fournisseurs de services Internet? Convierait-il, d’après vous, de les réglementer? Ce serait un moyen d’assurer qu’ils se comportent honnêtement et font effectivement ce qu’ils affirment faire. Vous avez dit également que certains FSI pourraient décider d’intervenir collectivement.

M. MacKay : Tout à fait. Ça ne se limite pas à un seul ordinateur. Une organisation criminelle peut exploiter tout un réseau.

Le sénateur Watt : Pourriez-vous me dire ce qu’il nous faudrait faire d’autre? Quelle autre solution recommandez-vous? Vous critiquez le projet de loi. Avez-vous quelque chose à proposer?

M. MacKay : Vous avez raison de me le demander. Ce que je propose, c’est la solution que j’ai avancée à la fin du plus long de mes deux exposés. J’y évoque l’idée d’un groupe tactique d’intervention en matière cybernétique. Cela nous ramène aux origines mêmes d’Internet. N’oubliez pas qu’il a été créé par le gouvernement des États-Unis, plus précisément par le ministère de la Défense. Ils l’ont organisé comme ils l’entendaient, étant donné qu’ils contrôlaient les subventions de recherche attribuées aux universités et aux divers instituts qui l’ont développé. Il y avait alors, au sein du système, de la cohérence et un certain nombre de règles techniques que chacun devait observer sous peine d’être exclu du réseau. Au fur et à mesure qu’Internet s’est développé, c’est devenu un peu une foire d’empoigne. Cela ne veut pas dire cependant qu’on ne puisse pas parvenir à s’autoréglementer. Internet est déjà régi par un certain nombre de règles techniques. La solution consisterait à les faire respecter. Il faudrait ainsi mettre en place un organisme au sein duquel travailleraient des gens qui connaissent bien le milieu. Si je contrôlais le routeur de pare-feu, je pourrais mettre fin à tout cela d’un instant à l’autre. Je dis ça en réponse à ce que le sénateur Runciman disait tout à l’heure au sujet des FSI qui se

want to relay it. It then passes through your networks to other people. I could shut this down easily as long as I had my finger on the button effectively.

You mentioned the CRTC. Frankly, that is the older technology. This is not a broadcast medium. It is something else and something that needs to be met on its own terms. I propose a computer emergency response team and so do all the experts on the cyber war threat to Canada, which is another issue not related to this bill.

Senator Angus: My understanding of the reason you are here is to say that this bill is not necessary, and will not do any good in protecting our children from these kinds of criminal activities we have been talking about because the law, as it stands, is adequate to do what is necessary. This bill adds nothing. That is what I understand. I read your document. You say that you do not need any change in the law to set up a CERT because you can set up a CERT under the present law. Do I have that right? In other words, you are saying that we are whistling past the graveyard with Bill C-22.

Mr. MacKay: I think so. There would be regulatory needs because we have to have some kind of obligation to ISPs to pay attention to the CERT; otherwise, what good is it? A rule of thumb in security is: You are not doing any good unless you have the power to enforce your rules. It needs to be something that works with them at their own level, such as a CERT. They are stakeholders in this thing. They want well-regulated networks. They do not want the reputation of this stuff showing up. They do not want to be punished under this bill. That is why I came to this conclusion.

Senator Angus: Is CERT your term?

Mr. MacKay: CERT is computer emergency response team. That term has been around for well over 20 years.

Senator Angus: I understand.

The Chair: This is frustrating, but we have to do what we have to do.

[Translation]

Senator Boisvenu: I am not a computer specialist, far from it, but I believe I understood the gist of your argument. You are saying that, instead of helping the system administrators do their work, the bill acts with you as paid officers of the state.

montreraient rétifs. La solution consiste à intervenir auprès d'eux au niveau technique. Le groupe tactique d'intervention n'aurait qu'à dire : écoutez, n'hébergez pas ce trafic, ne le relayez pas. Il transite par vos réseaux. Si j'avais mon doigt sur l'interrupteur, je pourrais facilement y mettre fin.

Vous avez parlé du CRTC. Je dois dire que là, il s'agit d'une technologie plus ancienne. Internet n'est pas un moyen de radiodiffusion. C'est quelque chose d'autre qui exige des modalités d'intervention spécifiques. Je propose donc la création d'un groupe tactique d'intervention cybernétique, ce que recommandent d'ailleurs tous les spécialistes des menaces cybernétiques qui pèsent sur le Canada, mais ça, c'est un autre problème.

Le sénateur Angus : Selon vous, donc, ce projet de loi n'est pas nécessaire et ne permettra pas de protéger nos enfants contre les activités criminelles en question, car la législation actuelle suffit à cet égard. Ce projet de loi n'ajouterait par conséquent rien. C'est comme cela que j'interprète ce que vous avez dit. J'ai lu votre exposé. D'après vous, il n'est pas nécessaire, pour créer un groupe tactique d'intervention cybernétique, de modifier la législation actuelle, car elle autorise déjà une telle mesure. Est-ce exact? Autrement dit, d'après vous, ce projet de loi n'a pas la moindre utilité.

M. MacKay : C'est effectivement ce que je pense. Ce qui serait nécessaire c'est de renforcer la réglementation, car il faudra bien imposer aux FSI l'obligation d'obtempérer aux instructions du groupe tactique d'intervention, sans cela à quoi servirait-il? En matière de sécurité, un bon principe à se rappeler est que vous ne faites rien de bon si vous n'avez pas les moyens de faire respecter la réglementation. Or, celle-ci doit, comme ce serait le cas d'un groupe tactique d'intervention, intervenir au niveau même des FSI, c'est-à-dire au niveau technique. Ils sont, en cela, parties prenantes. La réglementation des réseaux est dans leur intérêt. Ils ne veulent pas qu'on dise qu'ils tolèrent ce genre de matériel. Ils ne veulent pas être sanctionnés aux termes des dispositions du projet de loi. Voilà pourquoi j'en suis arrivé à cette conclusion.

Le sénateur Angus : L'expression groupe tactique d'intervention en matière cybernétique est-elle de votre cru?

M. MacKay : Non, l'expression existe depuis plus de 20 ans.

Le sénateur Angus : Je vois.

La présidente : Tout cela est un peu décourageant, mais il nous faut bien poursuivre notre examen de ce texte.

[Français]

Le sénateur Boisvenu : Je ne suis pas spécialiste en informatique, loin de là. Mais je pense que j'ai compris le cœur de votre argumentation. Vous dites qu'au lieu d'aider les administrateurs de systèmes à faire leur travail, le projet de loi consiste à agir avec vous comme des agents non rémunérés de l'État.

It is as though the Senate's Internet site and pornographic sites were the same thing. We know that pornographic sites are very hard to detect and that an average person cannot access them. They are very often networks.

Your participation and cooperation are essential. You say on page 3 that the bill gives you the impression that you are conspiring with pornographers and, at the end of your brief, you offer two ways to prevent the bill from applying or for circumventing the law. I call that conspiring.

Are you not using your brief to provide the people who distribute Internet services with a method for conspiring against the government?

[English]

Mr. MacKay: Is not the obligation of every citizen to avoid violating the law? The best way to avoid violating the law is not to fall afoul of its provisions. I just pointed out logically that, if the law applies to Internet service providers and you are not one, then the law would not apply to you. That is a logical point. The law talks about being advised. If you are not advised, then it does not apply to you. I just think it is an ordinary point about reasonable people not doing things that would lead them to fall afoul of the law. If they are in these circumstances, then of course they should respect it. I do not see that as plotting or so on. I do not see the language of the bill as aiding ISPs or treating them as partners, since it talks about fines if they do not do reporting of certain pieces of information. I see it as something slightly threatening and that a reasonable person would want to avoid falling under that circumstance.

Senator Chaput: At Parliament, we all have Internet services provided by Bell. If this bill goes through, is Bell responsible for reporting if something happens in one of our Internet services?

Mr. MacKay: I do not know. The answer to the question is, I do not know because I am not clear about what the bill means by the Internet service provider. Is it your own network? Is it Bell? I am not sure.

Senator Chaput: You do not know.

Mr. MacKay: I do not know.

Senator Chaput: Thank you.

The Chair: Mr. MacKay, we have had a cultural encounter here. There are two different worlds. I must say you have managed to drag us kicking and screaming into something approaching a beginner's understanding of your world and your perspective. That is a major accomplishment, and we thank you very much for doing that. We appreciate it.

Mr. MacKay: Thank you for the opportunity.

Comme si de comparer le site Internet du Sénat et le comparer aux sites pornographiques serait du même niveau. Nous savons que les sites pornographiques sont des sites très difficiles à détecter, et que ce n'est pas monsieur et madame tout-le-monde qui ont accès à cela. Il s'agit souvent de réseaux.

Votre participation et votre collaboration sont essentielles. Vous dites à la page 3 que le projet de loi vous donne l'impression que vous complotez avec les auteurs de la pornographie et, à la fin de votre mémoire, vous donnez deux trucs pour ne pas que la loi s'applique ou pour contourner la loi. Moi, j'appelle cela comploter.

Est-ce que vous ne donnez pas la recette dans votre mémoire, aux gens qui distribuent des services Internet, à savoir comment comploter contre le gouvernement?

[Traduction]

M. MacKay : Chaque citoyen n'est-il pas tenu au respect de la loi? Or, le meilleur moyen d'éviter d'enfreindre la loi est d'en respecter les dispositions. Je viens de faire remarquer que dans la mesure où la loi s'applique aux fournisseurs de services Internet, si vous n'êtes pas fournisseur de service Internet, la loi ne s'applique pas à vous. C'est logique. Le projet de loi parle d'une personne qui est « avisée » de quelque chose. Si donc, vous n'avez pas été avisé, la loi ne s'applique pas à vous. Cela n'a rien d'extraordinaire, je parle là uniquement de personnes raisonnables qui ne font rien pour se mettre en infraction. Si, elles se retrouvent en pareille situation, il est clair qu'il leur faudra respecter les dispositions applicables. Je ne parle aucunement de comploteurs. C'est simplement que les dispositions de ce projet de loi ne me semblent pas aider les FSI, ni les considérer comme des partenaires, étant donné qu'il est immédiatement question des amendes auxquelles ils s'exposent s'ils ne communiquent pas certains renseignements. Il y a en cela quelque chose de menaçant qu'une personne raisonnable souhaiterait éviter.

Le sénateur Chaput : Les services Internet auxquels nous avons, nous parlementaires, accès sont fournis par Bell. À supposer que ce projet de loi soit adopté, Bell sera-t-elle tenue de faire la déclaration prévue si ce genre de chose se produit dans le cadre de nos services Internet?

M. MacKay : Je ne sais pas. Je dois vous répondre que je ne sais pas, car je ne vois pas ce que le projet de loi entend au juste par fournisseur de services Internet. Est-ce votre réseau? Est-ce Bell? Je ne suis pas sûr.

Le sénateur Chaput : Vous ne savez pas.

M. MacKay : Je ne sais pas.

Le sénateur Chaput : Je vous remercie.

La présidente : Monsieur MacKay, c'est une véritable rencontre interculturelle que nous avons eue aujourd'hui. Ce sont deux mondes différents. Je dois dire que vous êtes parvenu à nous entraîner à nos corps défendants et à nous inculquer une certaine compréhension du monde dans lequel vous évoluez. C'est tout de même quelque chose, et nous vous en remercions sincèrement.

M. MacKay : Je vous remercie de m'en avoir donné l'occasion.

The Chair: Turning to our last panel this evening, we have two witnesses from whom we are privileged to hear. From UNICEF Canada, we have Marvin Bernstein, Chief Advisor, Advocacy, and from Kids Internet Safety Alliance, we have Paul Gillespie, President and Chief Executive Officer. Mr. Bernstein, you have the floor.

Marvin Bernstein, Chief Advisor, Advocacy, UNICEF Canada: Thank you for the invitation on behalf of UNICEF Canada. UNICEF Canada strongly supports the enactment of Bill C-22 in principle as being a timely piece of legislation and a positive step towards achieving greater child protection and safety, certainly consistent with the provisions contained in the United Nations Convention on the Rights of the Child.

We take the position that it is clear that the sexual abuse of children is being facilitated by digital technologies and that children have rights to protection from sexual abuse in all of its forms. Bill C-22 is a step forward in the protection of Canada's children. However, a full, rights-based and systems approach to child protection suggests the need for some amendments to Bill C-22, or the establishment of guidelines that could enhance the prevention of risk for all children. The amendments we propose recognize that children are not only victims of sexual abuse, but also engage in risk behaviours that cause harm to themselves and other children in the use of digital technologies. To protect all children from harm, children need to know what constitutes abusive and illegal activity, how to report it, and how to avoid actions that would harm other children and themselves.

To strengthen the objectives of the bill, it is important, in our view, to address three areas: First, the absence of a statement of purpose provision; second, the mitigation of exposure of children and youth to criminal charges and prosecution; and, third, the need for children and youth to receive preventive and corrective education.

One of the recommendations is that the bill be amended to add a new section enumerating the main purposes of the bill. Recommendation number 2, which I will not go through, is that consideration be given to including in this new statement of purpose provision a set of purposes. We have defined what some of those purposes could be by way of illustration.

Around the mitigation of exposure of children to criminal charges and prosecution, while we applaud the laudable purposes of Bill C-22 in promoting the online protection and safety of children, we are concerned about the unintended consequence of children and youth being subject to greater exposure to criminal liability and prosecution through the projected increased

La présidente : Nous abordons maintenant notre dernier panel. Nous accueillons avec plaisir nos deux témoins. Il s'agit, au nom d'UNICEF Canada, de Marvin Bernstein, conseiller principal de la promotion et de la défense des droits, et, représentant la Kids Internet Safety Alliance, de Paul Gillespie, président et directeur général. M. Bernstein, vous avez la parole.

Marvin Bernstein, conseiller principal, Promotion et défense des droits, UNICEF Canada : Au nom d'UNICEF Canada, je tiens à vous remercier de l'occasion qui nous est ainsi donnée de prendre la parole devant vous. UNICEF Canada est un fervent partisan de l'adoption du projet de loi C-22, qui représente, à ses yeux, une disposition à la fois opportune et constructive au niveau de la protection et de la sécurité de l'enfance. Les mesures proposées se situent tout à fait dans la ligne de la Convention des Nations Unies relative aux droits de l'enfant.

Il est selon nous évident que les technologies numériques facilitent l'exploitation sexuelle des enfants et que les enfants ont le droit d'être protégés contre la maltraitance sexuelle sous toutes ses formes. Le projet de loi C-22 représente une avancée pour la protection des enfants au Canada. Si, cependant, l'on envisage la protection des enfants dans le cadre d'une approche systémique fondée sur une reconnaissance intégrale de leurs droits, on s'aperçoit que le texte appelle un certain nombre d'amendements, ou l'adoption de lignes directrices permettant de prévenir plus efficacement qu'à l'heure actuelle les risques auxquels sont exposés les enfants. Les amendements que nous proposons reconnaissent non seulement que les enfants sont effectivement victimes de maltraitance sexuelle, mais que dans leur utilisation des technologies numériques, ils ont parfois des comportements à risque qui peuvent leur causer préjudice, à eux ainsi qu'à d'autres enfants. Si l'on entend protéger tous les enfants, il faut leur apprendre à reconnaître ce qui constitue une activité abusive et illicite, leur enseigner comment signaler de telles activités et comment éviter les comportements qui les mettent en danger, eux et d'autres enfants.

Il conviendrait d'après nous, afin de renforcer le but que vise le projet de loi, d'adopter trois mesures : d'abord, formuler un exposé des objectifs du projet de loi; deuxièmement, atténuer les risques de voir des enfants et des adolescents accusés d'une infraction pénale, et poursuivis; et troisièmement, assurer aux enfants et aux adolescents la nécessaire éducation préventive et corrective.

Nous recommandons notamment que le projet de loi soit modifié en y incorporant un nouvel article exposant les principaux objectifs du texte. Je ne vais pas détailler notre deuxième recommandation, mais elle consiste à intégrer à cet exposé des objectifs, une énumération détaillée de ceux-ci. Nous avons, à titre d'illustration, défini certains des objectifs qu'il conviendrait d'y faire figurer.

Nous nous félicitons du but que vise le projet de loi C-22 et qui consiste à renforcer la protection et la sécurité des enfants dans leur emploi d'Internet, mais nous craignons que ces dispositions entraînent, pour les enfants et les adolescents, des conséquences peu souhaitables en augmentant le risque de les voir faire l'objet de poursuites pénales dans la mesure où l'on oblige les

reporting by Internet service providers of the digital activity of such young persons, where it involves sexual abuse images. This heightened exposure to criminal liability may occur even when actions reflect a youthful exploratory instinct or a lack of awareness of the consequences and have no malicious intent.

As such, there are heavy and disproportionate consequences that may accrue to young people for not knowing the legal parameters of the responsible use of technologies. I am talking about sexting here and transmitting messages — it could be videos and photographs that are sexually explicit — between young people themselves. It is important to be vigilant, in our estimation, that in our focus, which is an important focus, to protect children from the possession, transmission and accessing of sexual abuse images, that we do not inadvertently create legislative machinery that could be used to hurt children in other ways.

It is also necessary to consider the risks to children and youth whose actions are criminalized when transmitting sexual images, or otherwise accessing website and other digital child pornographic content, as defined in section 163.1 of the Criminal Code. Such criminalization could lead to reputational damage, a permanent stigma negatively affecting education and employment opportunities, and potential acts of self harm resulting from a sense of embarrassment or humiliation.

I will not go through this, but in our brief we submitted some observations and analysis from *R. v. Sharpe*, the Supreme Court of Canada decision in 2001. To move on, our recommendations are that police charging guidelines and prosecutorial guidelines be developed that could be used to withdraw charges or to stay criminal proceedings, in the case of prosecutorial guidelines, against a child who may have technically committed an offence under section 163.1 of the Criminal Code.

We also recommend, in our fourth recommendation, that a list of non-exclusive factors be identified for Crown attorneys to consider when determining whether to prosecute a child for committing an offence under section 163.1 of the Criminal Code. Again, by way of illustration, we identify some possible factors that could be encouraged.

By way of justification, our legal analysis suggests that children and youth may be charged or prosecuted for technical breaches of section 163.1 of the code, and may not be able to rely upon considerations of consent or private possession or use, particularly where there has been the distribution or transmission of child pornography under subsection 161.1(3), which is the transmission or distribution offence; or the accessing of child pornography by the recipient under subsection 163.1(4.1) of the code, which is the accessing the child pornography offence.

fournisseurs de services Internet à signaler ces jeunes personnes, à chaque fois qu'elles visionnent des images de maltraitance sexuelle. Cette responsabilité pénale accrue risque d'être engagée même lorsque les actes en cause sont simplement le reflet d'une curiosité juvénile, ou d'un manque de compréhension des conséquences que cela peut avoir et ne répondent à aucune intention délictueuse.

Le simple fait d'ignorer les règles de droit régissant un emploi responsable des nouvelles technologies risque donc d'entraîner pour les jeunes des conséquences graves et disproportionnées. Je pense là aux sextos, c'est-à-dire à la transmission, entre adolescents, de vidéos ou de photographies sexuellement explicites. Il faut selon nous veiller, certes, à protéger les enfants contre la possession, la transmission et la consultation de représentations graphiques d'exploitation sexuelle, mais veiller en même temps à ce que les dispositions législatives que nous mettons en œuvre n'entraînent pas d'autres sortes de préjudices.

Il ne faut pas perdre de vue les risques auxquels sont exposés les enfants et les jeunes dont on incrimine le comportement lorsqu'ils transmettent des photos sexuellement explicites, ou consultent des sites web ou d'autres contenus numériques constituant de la pornographie juvénile au sens de l'article 163.1 du Code criminel. Une telle criminalisation de leur comportement est de nature à nuire à leur réputation, et à les stigmatiser durablement avec tous les risques que cela comporte, d'abord pour leur éducation, puis pour leur vie professionnelle. L'humiliation que cela peut leur infliger pourrait en outre les porter à des actes autodestructeurs.

Je ne vais pas entrer dans le détail, mais nous avons incorporé à notre mémoire des raisonnements et analyses tirés de l'arrêt rendu par la Cour suprême du Canada en 2001 dans l'affaire *R. c. Sharpe*. Nous recommandons l'élaboration de lignes directrices régissant les pratiques des policiers et des procureurs de la Couronne, en matière d'accusations afin de faciliter le retrait des accusations ou la suspension des procédures criminelles engagées contre un enfant qui aurait, au sens strict, effectivement commis une infraction à l'article 163.1 du Code criminel.

Quatrièmement, nous recommandons qu'une liste de facteurs non exclusifs soit transmise aux procureurs de la Couronne afin d'orienter leurs décisions lorsqu'ils envisagent de poursuivre un enfant pour infraction à l'article 163.1 du Code criminel. Là encore, à titre d'exemple, nous avons énuméré un certain nombre de facteurs dont il y aurait lieu de tenir compte.

Nous estimons, en effet, que les enfants et les adolescents pourraient être accusés, ou poursuivis, pour ce qui serait effectivement, au sens strict, des violations de l'article 163.1 du Code, dans des circonstances ne leur permettant pas d'invoquer, par exemple, l'absence de consentement, ou le caractère privé de la possession ou de l'utilisation des documents en cause, notamment lorsqu'il y a eu distribution ou transmission de pornographie juvénile selon le paragraphe 161.1(3) du Code, ou lorsque l'intéressé accède à de la pornographie juvénile contrairement au paragraphe 163.1(4.1).

This would then place young persons at risk of criminal liability in the case of their sending or receiving sexually explicit messages, photos or videos. Accordingly, a reasonable response to this risk of criminalization would be the development of appropriate police charging and Crown attorney prosecutorial guidelines.

The last area, briefly, is the provision of preventive education for children. To protect all children from abuse, children need to know what constitutes abusive and illegal activity to know how to report it and to avoid actions that would harm other children and themselves. We see the need for increased education to prevent children from being placed at risk of abuse, and also at risk of criminal prosecution.

The bill offers an opportunity to press for the need for preventive education of youth — that is all youth — through effective programs that consult youth in their design and are properly evaluated. In this regard, preventive education would benefit not only potential youth victims, but also potential youth victimizers who may not fully appreciate the implications of their actions.

We need to recognize that not all children receive the same quality of parenting and the same kind of guidance. This kind of preventive education in terms of identifying the risks — what are the implications of engaging in this kind of activity — is quite crucial to try to structure and organize around the same time as the bill is proclaimed. In the submission, we have identified a number of different websites that have the potential within Canada, from abroad, that provide this kind of preventive information to young people.

The recommendation in this area, number five, is that Bill C-22 be amended, or regulations thereto and/or guidelines be created, to require the development and dissemination of effective educational interventions for children and young people to address the risks involved in making, possessing, transmitting or accessing child pornography, as defined by the Criminal Code.

Last, there should be due consideration of the recommendations for training, education and public awareness advanced by the Canadian Centre for Child Protection, as a result of the review of the Manitoba experience with mandatory reporting of child pornography.

The last point I want to make is that we have some statistical information from Europe that illustrates that sexting goes on more frequently than we would think. This generally tends to be communications between young people themselves, between boyfriend and girlfriend.

Les jeunes qui envoient ou qui reçoivent des photos ou vidéos sexuellement explicites ou des sextos, s'exposent actuellement à une accusation pénale. Il serait raisonnable, compte tenu de ce risque de criminalisation, d'élaborer à l'intention de la police et des procureurs de la Couronne, des lignes directrices en ce domaine.

Très brièvement, le dernier point concerne l'éducation préventive des enfants. Si l'on veut protéger les enfants contre l'exploitation et la maltraitance, il faut faire en sorte qu'ils sachent ce qui constitue une activité abusive et illicite, qu'ils sachent comment signaler ce type d'activité et comment éviter les comportements susceptibles de faire du tort, tant à eux-mêmes, qu'à d'autres enfants. Il nous semble essentiel d'accroître nos moyens d'éducation afin d'éviter aux enfants à la fois les risques d'exploitation, et les risques de poursuites pénales.

Ce projet de loi est l'occasion d'insister sur le besoin d'assurer à tous les jeunes une éducation préventive par des programmes efficaces, à la conception desquels les jeunes seraient appelés à participer. Je dois dire que cette éducation préventive servira non seulement les jeunes victimes potentielles, mais également leurs agresseurs qui ne comprennent peut-être pas toujours très bien les conséquences de leurs actes.

Il nous faut tenir compte du fait que tous les enfants ne reçoivent pas de leurs parents les mêmes soins et la même éducation. Il est donc essentiel, je pense, d'organiser et de mettre en œuvre ce type d'éducation préventive au moment même où le projet de loi entrera en vigueur afin de mieux cerner les risques et les conséquences du type d'activité en cause. Dans le cadre de notre mémoire, nous avons indiqué, tant au Canada que dans d'autres pays, divers sites Internet susceptibles d'assurer aux jeunes ce genre d'éducation préventive.

Nous proposons, dans le cadre d'une cinquième recommandation, que le projet de loi C-22 soit modifié, ou que soient adoptées une réglementation et/ou des lignes directrices prévoyant l'élaboration et la mise en œuvre, à l'intention des enfants et des adolescents, de mesures éducatives efficaces. Il s'agit de leur faire prendre conscience des risques auxquels les exposent ceux qui produisent, possèdent ou transmettent de la pornographie juvénile, telle que définie dans le Code criminel, ou qui accèdent à ce matériel.

Et, en dernier lieu, il convient de prendre pleinement en compte les recommandations formulées par le Centre canadien de protection de l'enfance, recommandations formulées suite à l'examen des résultats obtenus au Manitoba après l'adoption de dispositions concernant la déclaration obligatoire des cas de pornographie juvénile.

Enfin, je voudrais faire état de certaines statistiques européennes indiquant que le sexting est beaucoup plus fréquent qu'on ne le penserait. Il s'agit d'ailleurs, en général, de communications entre adolescents, notamment entre copains et copines.

The real purpose of this bill is to try and prevent predators from engaging in serious sexual abusive acts and victimizing young children with inappropriate activities. It is not to catch or capture this kind of curious or rather benign communications between young people. It is an unintended consequence, and there is a bit of a blind spot because of this gap in the Criminal Code that does not really capture or set out these exceptions in the case of transmissions and accessing child pornography.

The Supreme Court of Canada decision speaks to possession and making of child pornography. At the time that section of the code was enacted and the *Sharpe* case was decided, there was not this level of digital activity and people were not as proficient.

I heard the previous presenter. I fall into your side of the table and do not have the technological expertise. My background is in child protection. I was a provincial children's advocate in Saskatchewan for five years and I now work at UNICEF.

This bill is absolutely necessary to try to eradicate an escalating situation that is wreaking havoc and is harmful to children. However, there is another contextual element here that needs to be considered so we do not inadvertently create other problems for young people. I will stop there.

The Chair: Necessary but not sufficient, would that be a summary?

Mr. Bernstein: Yes. Thank you.

Paul Gillespie, President and Chief Executive Officer, Kids Internet Safety Alliance: As I am the last speaker, I will not be long, but prior to the questions I would like to provide a bit of context for your thoughts with regard to these Internet discussions.

I was a police officer in Toronto for 28 years and I left the Toronto police force in 2006. In my last six years, I was the officer in charge of the child exploitation section. I had a great team of officers who developed some of the ground-breaking techniques still being used around the world today.

In 2002, I was invited to make a presentation at an all-party meeting in Parliament to discuss child exploitation and the impacts of the Internet. In 2003, I was asked to return to have a similar meeting with the Conservative caucus.

Regarding the system you mentioned earlier, CETS, the Child Exploitation Tracking System that is being used across Canada and now around the world, I am the one who contacted Microsoft and helped build the system. I am still involved with maintaining it and trying to spread the word that we need to work together. I just wanted to give you a bit of background about who I am.

Ce projet de loi vise à empêcher les prédateurs de se livrer à des sévices sexuels et de victimiser de jeunes enfants. Il ne s'agit pas en effet de réprimer les communications sexuellement explicites relativement anodines que peuvent s'échanger les jeunes. Ce serait une conséquence due à une sorte de lacune au Code criminel qui ne fait place à aucune exception en matière de transmissions ou d'accès à la pornographie juvénile.

L'arrêt de la Cour suprême du Canada concerne la possession et la production de pornographie juvénile. Or, à l'époque où a été adoptée cette disposition du Code, et rendu l'arrêt *Sharpe*, l'activité numérique était beaucoup moins développée et les gens n'étaient en général pas aussi compétents en ce domaine.

J'ai écouté ce qu'a dit le témoin précédent. Je fais partie de ceux qui ne possèdent pas ce bagage technologique. Mon domaine est la protection de l'enfance. Pendant cinq ans, j'ai été, en Saskatchewan, protecteur des enfants, et maintenant je suis à l'UNICEF.

Ce projet de loi est nécessaire si nous voulons empêcher que ne s'aggrave une situation qui fait déjà des ravages parmi les enfants. Cela dit, il faut également tenir compte du contexte afin de ne pas, en même temps, engendrer chez les jeunes des problèmes supplémentaires. Je vais m'en tenir là.

La présidente : Nécessaire mais non suffisant, est-ce une assez bonne manière de résumer la question?

M. Bernstein : En effet. Je vous remercie.

Paul Gillespie, président-directeur général, Kids Internet Safety Alliance : Je suis le dernier intervenant et je m'en tiendrai donc à l'essentiel. Avant que nous passions aux questions, cependant, je tiens à apporter quelques précisions au sujet du contexte dans lequel se situe ce débat.

J'ai été, pendant 28 ans, policier à Toronto. J'ai quitté la police de Toronto en 2006. Pendant mes six dernières années dans la police, j'étais chargé de la section de lutte contre l'exploitation des enfants. J'étais entouré d'une excellente équipe de policiers et, ensemble, nous avons découvert de nouvelles méthodes qui sont, aujourd'hui encore, employées dans le monde entier.

En 2002, j'ai été invité à l'occasion d'une réunion de tous les partis qui se tenait au Parlement, à présenter un exposé sur l'exploitation des enfants et le rôle d'Internet. En 2003, on m'a demandé de prendre à nouveau la parole à l'occasion d'une réunion du caucus du Parti conservateur.

Je peux dire, en ce qui concerne le système dont vous avez parlé tout à l'heure, c'est-à-dire le CETS, le système d'analyse contre la pornographie juvénile, employé partout au Canada, et maintenant dans divers pays du monde, que c'est moi qui ai contacté Microsoft et aidé à mettre sur pied ce système. Je continue à contribuer à son avantage unir nos efforts. Je tenais simplement à vous dire quelques mots de mes antécédents.

In 1997, I was involved in an investigation of something called “The Wonderland Club.” This is a group of worldwide predators who, for the first time, were seen using the Internet to basically host pay-per-view child abuse. It was horrible. They were all over the world.

It was first identified in California. A global investigation of some very smart people, similar to the previous guest, identified that the real bad guys were centred out of England.

The police got involved and they actually arrested one of the main bad guys. When they did so, they took over his identity in an undercover capacity in the same way you would infiltrate a drug ring. When he got onto the computer, posing as the person arrested, he started to chat and pretend he was that man. He had spent the last month learning everything there was to know.

Within five seconds of him starting to type, his screen went black. At that time, that group had a bot monitoring the group and it identified the fact that this particular chat was coming from a different IP address, one that had never been used before by this individual. It sensed a threat and moved the group to another location. This was in 1997. To this day, that is still quite remarkable.

In 2003, I was involved in an investigation of something called the Darknet or the Freenet. This was the bowels of the Internet where the worst of the worst bad guys operate. It was originally developed by some MIT, Massachusetts Institute of Technology, grads who were concerned about the ability of students in some areas of world to be able to communicate and have free speech. They built something, thinking that it will never be able to be traced to the authors and, in fact, they were right. They did a great job. It still operates. However, like all other technology, when the bad guys see something, they are the first to modify it for their own use.

The investigation that we conducted from 2003 to 2006 was the most mind-numbing thing I have ever seen in my life. These were the predators — the worst of the worst — in the tens of thousands who produce the really vile stuff that is disbursed through the Internet.

We are now 2011, so those particular investigations were 8 and almost 15 years ago. That is the sophistication that is out there today. I think you need to keep that in mind as you consider this and future Internet-based legislation.

First, I would say that I absolutely think this legislation is good. I echo the sentiments of most others here in thinking that there should be a responsibility placed upon service providers. I was around back when there were some challenges. I think most

En 1997, j’ai participé à une enquête sur un groupe qui s’appelait « The Wonderland Club. » Il s’agissait d’une bande de prédateurs habitant divers pays du monde qui, pour la première fois, offrait, par le truchement d’Internet, un service de pornographie juvénile à la carte. C’était quelque chose d’atroce. Ils étaient installés un peu partout dans le monde.

On en a d’abord repéré en Californie. Une enquête mondiale menée par des gens très intelligents, un peu comme votre témoin précédent, ont permis de découvrir que les vrais responsables étaient installés en Angleterre.

La police est intervenue et a arrêté un des principaux responsables. L’arrestation opérée, un des enquêteurs a assumé l’identité du prévenu dans le cadre d’une opération d’infiltration comme s’il s’agissait de s’infiltrer dans un réseau de trafiquants de drogue. Assumant, sur Internet, l’identité du personnage arrêté, l’agent commença à converser, se faisant passer pour l’autre. Il lui avait fallu un mois pour composer son personnage.

Son écran s’est obscurci soudainement, à peine cinq secondes après qu’il eut commencé à taper sur son clavier. Le réseau avait, en effet, installé un bot informatique qui lui permit de savoir que ce clavardage provenait d’une adresse Internet différente, d’une adresse que l’autre n’avait jamais employée. Le groupe a perçu la menace et s’est installé ailleurs. Ça, c’était en 1997. La manœuvre employée à l’époque demeure assez remarquable.

En 2003, j’ai pris part à une enquête sur un réseau appelé Darknet ou Freenet. Ce réseau se situait dans les boyaux d’Internet, là où opèrent les malfaiteurs les plus dangereux. Il s’agit d’un réseau mis au point à l’origine par des diplômés du Massachusetts Institute of Technology, qui souhaitaient donner aux étudiants de certains pays les moyens de communiquer et de s’exprimer librement. Ils ont créé ce réseau, pensant qu’on ne pourrait jamais remonter jusqu’à eux, ce qui était effectivement le cas. Ils ont fait du bon travail et, de fait, ce réseau fonctionne toujours. Comme pour tous les moyens techniques, cependant, lorsque des êtres malfaisants cherchent à s’accaparer quelque chose de bien, ils commencent par l’adapter à leurs propres besoins.

L’enquête que nous avons menée de 2003 à 2006 a révélé des choses proprement hallucinantes. Il s’agissait de prédateurs — les plus mauvais parmi les mauvais — qui par dizaines de milliers produisent quelque chose de vraiment dur qu’ils distribuent ensuite sur Internet.

Les enquêtes dont je viens de faire état ont été menées respectivement il y a 8 et presque 15 ans. C’est dire le niveau technique auquel on se heurte. Je pense que c’est un facteur dont vous devez tenir compte lorsque vous envisagez d’adopter des dispositions législatives concernant Internet, que ce soit aujourd’hui ou à l’avenir.

Je vais dire, d’abord, que ce projet de loi me paraît être une excellente chose. Comme la plupart des personnes ici présentes, j’estime en effet qu’il convient de placer les fournisseurs de services devant leurs responsabilités. J’ai pu, dans le passé,

service providers are doing the right things for the right reasons. I believe that they will call, but let us ensure they do. That inherent responsibility needs to be placed on them.

My organization is called KINSA, Kids Internet Safety Alliance, and I started this when I left the police force. Our mandate is simple: To find and rescue these poor kids whose images are being shared on the Internet. You have probably heard many different numbers over the course of this particular endeavour as to how many pictures and kids are out there. The reality is that we only know about 2 per cent of the children whose images are being transferred around the world.

My organization trains cyber cops from developing nations to do a better job on the Internet, to better identify and rescue these kids, and to raise their bars a little so they can join the likes of the great officers we have in Canada and elsewhere within the RCMP, the OPP, the FBI and Interpol. Today, we have trained officers from 10 different countries, such as Romania, Chile, Brazil, Malawi, Mozambique and Zambia.

One of the Brazilian officers, once trained, actually led to the identification and arrest of an offender in a small town called Tracyville, New Brunswick. The offender had been abusing 10 kids. This was in the papers last week. The offender pled guilty. Had that officer from Brazil not received that training, those kids would not have been identified and rescued.

I want to let you know this because there are often thoughts that we need to have 10, 100, 1,000 or 10,000 more cyber cops out there and I suggest it is not realistic, based on the taxes and the cost.

The reality is the Internet has no borders. Therefore, we are positioned such that there are tens of thousands of cyber cops working around the world right now. They are keen, eager, young police officers — the Romanian National Police, the Polish National Police, the Brazilian Federal Police — who patrol the Internet. However, they are only really allowed to work on credit card fraud or eBay fraud. They are not quite sensitized enough to recognize that they could also be doing other things out there.

Therefore, that is what we are doing. It is very expensive to plant the seed, water it and wait five years for it to grow. That is what we are doing when we are hiring and training new cyber cops. I am trying to plant the seeds that are already growing around the world, and explain that they need to pay attention to kids who might be in your country or who might be somewhere else.

constater un certain nombre de difficultés à cet égard, mais je pense que la plupart des fournisseurs de services n'hésitent pas à prendre leurs responsabilités, estimant que c'est effectivement la chose à faire. Je pense donc qu'ils signaleront effectivement les cas dont ils ont connaissance. Il nous faut néanmoins veiller à ce qu'ils le fassent en leur imposant cette responsabilité.

L'organisation à laquelle j'appartiens s'appelle KINSA, Kids Internet Safety Alliance. Je l'ai lancée à l'époque où j'ai quitté la police. Notre mission est simple : retrouver et sauver les enfants dont les photos circulent sur Internet. Sans doute vous a-t-on cité divers chiffres concernant le nombre de photos et d'enfants impliqués. Le fait est que nous ne sommes au courant que d'environ 2 p. 100 des enfants dont les images sont diffusées à travers le monde.

Mon organisation assure la formation des cybergendarmes de pays en développement, leur enseignant comment travailler plus efficacement sur Internet, et comment parvenir à mieux identifier et récupérer ces enfants. Nous tentons de relever le niveau afin qu'ils puissent travailler de concert avec les spécialistes policiers que nous avons ici au Canada et ailleurs, que ce soit au sein de la GRC, de la Police provinciale de l'Ontario, du FBI ou de l'Interpol. Nous avons jusqu'ici assuré la formation de policiers de 10 pays différents, dont la Roumanie, le Chili, le Brésil, le Malawi, le Mozambique et la Zambie.

Un des policiers brésiliens a réussi, à l'issue de sa formation, à identifier et à faire arrêter un délinquant installé à Tracyville, une petite ville du Nouveau-Brunswick. Cet individu avait maltraité 10 enfants. On en a parlé dans les journaux la semaine dernière. Il a plaidé coupable. Si ce policier brésilien n'avait pas reçu la formation en question, ces enfants n'auraient été ni identifiés ni mis en sûreté.

Je tenais à vous préciser cela, car les gens disent souvent qu'il nous faudrait déployer 10, 100, 1 000 ou 10 000 cybergendarmes de plus mais, compte tenu du niveau des impôts et des coûts que cela implique, pareille solution n'est guère réaliste.

Ce qui est vrai, c'est qu'étant donné qu'Internet n'a pas de frontières, nous sommes effectivement, à travers le monde, des dizaines de milliers de cybergendarmes qui unissent leurs efforts. Ces jeunes policiers enthousiastes qui patrouillent Internet, appartiennent à la Police nationale roumaine, à la Police nationale polonaise ou à la Police nationale du Brésil. On les oblige, cependant, à travailler uniquement sur la fraude à la carte de crédit ou à eBay. Ils ne sont pas encore suffisamment conscients du problème pour comprendre qu'ils pourraient s'attaquer à d'autres types de criminalité.

C'est à cela donc que nous consacrons nos efforts. C'est un travail coûteux et de longue haleine que de planter la graine, de l'arroser et d'attendre cinq ans pour qu'elle pousse. C'est pourtant ce que nous faisons lorsque nous engageons et que nous formons de nouveaux cybergendarmes. J'essaie de planter des graines de par le monde et d'expliquer pourquoi il faut s'occuper de ces enfants quel que soit leur pays d'origine.

This scourge and this deluge of awful we are in the middle of is bigger than anyone could have ever imagined. The numbers are shocking. Someday, the only way we will get rid of it will be through a technical solution, to segue to the previous speaker. It will certainly never be solved by human eyes.

I wanted to let you know that this is good legislation.

The one last piece I want to remark on is that, when we send officers back to their country with new techniques and ways to do business, we also send them back with the best practices of the law enforcement we have here in Canada. The officers we have as cyber cops are second to none. They are brilliant. I could not always say that, but I can now. We send not only our techniques but our legislation because we have some of the best laws in the world, certainly in the case of cyber laws. We should be proud of that.

I think this is another piece of legislation that is vital and necessary — I do not want to say “keeps us ahead of the curve.” As leaders in this area, we have responsibilities to share what we do best and I think we are starting to do that more.

There were comments earlier about whether there are enough people to handle this, whether there are enough police officers and whether they are ready for this onslaught. Time will tell whether there is a serious need for more officers.

However, one must consider the big picture, the amount of images being shared and the way that people are sharing them. Most of it is not being done through websites, but through file sharing, the way we download music. It would be like dropping you in the middle of Lake Ontario and asking you if you noticed if someone in Toronto threw another bucket of water in the lake. That is how swamped the officers around the world are right now. They will never get out from under that using the methods they are using now.

I want to thank you for the time. I laud the government for this legislation. I think it is good, and I would invite you to keep the conversations going because soon we will need to start talking bigger picture stuff. Thank you.

Senator Wallace: Thank you very much for the presentations.

Mr. Bernstein, the first question I direct to you. Both your written and oral presentations were comprehensive. You are looking at this issue very comprehensively, from the point of view of providing as much protection as possible to children who find themselves involved with this terrible, terrible problem.

I know from your comments you are well aware of this, but Bill C-22 is not perhaps as comprehensive and broad in its approach as what you describe. It is a very focused bill and deals specifically with the requirement for the mandatory reporting by

Ce véritable fléau a une ampleur qui dépasse tout ce qu'on aurait pu imaginer. Les chiffres sont faramineux. Il arrivera un jour où nous parviendrons, par des moyens techniques, à nous en débarrasser et je reprends là ce qu'a dit le témoin précédent. Il est certain qu'on ne parviendra jamais à régler le problème par des moyens purement humains.

Je tiens donc à vous assurer que ce projet de loi me paraît être une bonne chose.

Et puis, pour terminer, il me faut dire que lorsque les policiers que nous avons formés, rentrent dans leur pays d'origine, armés de nouvelles techniques et ayant appris notre manière de faire, ils ramènent également chez eux les pratiques exemplaires développées ici en matière de police. Nos cybergendarmes sont effectivement les meilleurs au monde. Ils sont, on peut le dire, brillants. Je n'ai pas toujours pu en dire autant, mais il m'est maintenant possible de l'affirmer. Nous n'exportons donc pas seulement nos techniques, mais également notre législation car, du moins dans le domaine cybernétique, notre législation est la plus avancée. C'est quelque chose dont nous pouvons être fiers.

Ce projet de loi est essentiel et nécessaire et j'allais le dire, nous donne une longueur d'avance. En tant que leaders dans ce domaine, il nous appartient de partager ce que nous faisons de meilleur et, je crois que nous faisons cela de plus en plus.

Quelqu'un a demandé, plus tôt, si les ressources policières actuellement engagées suffisent, si nos services sont prêts à faire face à ce fléau. Nous ne sommes pas encore en mesure de nous prononcer sur ce point.

Il ne faut pas, il est clair, perdre de vue l'ampleur du problème, le nombre d'images diffusées et les divers moyens employés pour cela. La diffusion ne se fait d'ailleurs pas essentiellement au moyen de sites Internet, mais par le partage de fichiers, comme pour la musique. Disons, pour mesurer l'ampleur du phénomène que c'est un peu comme si on vous lâchait au beau milieu du lac Ontario, et qu'on vous demandait si vous vous étiez aperçu qu'un habitant de Toronto venait de déverser un seau d'eau dans le lac. C'est un peu la situation dans laquelle se trouvent actuellement les policiers des divers pays. Ils n'y arriveront pas par les méthodes actuelles.

Je vous remercie de votre attention. Je félicite le gouvernement d'avoir présenté ce projet de loi. C'est un texte valable et je vous incite à entretenir le débat sur la question car, bientôt, il va nous falloir envisager des mesures plus globales. Je vous remercie.

Le sénateur Wallace : Nous vous remercions de votre exposé.

Monsieur Bernstein, c'est à vous que je souhaite poser ma première question. Vous nous avez fait parvenir un mémoire et vous nous avez présenté un exposé oral des plus complets. Je vois que vous avez sur la question un point de vue global et que vous vous attachez dans toute la mesure du possible à protéger les enfants qui se trouvent impliqués dans cet atroce trafic.

Je vois, d'après ce que je vous ai entendu dire, que vous êtes parfaitement conscient du fait que ce projet de loi n'est peut-être pas aussi étoffé que vous ne l'envisagiez. Il s'agit d'un texte ayant un objet très précis, en l'occurrence l'obligation, pour les

Internet service providers. It does not get into a review and possible revisions of section 163 of the Criminal Code of Canada, which is really where the meat of child pornography offences lies.

I believe I am stating the obvious in saying that it is fair to say, based on your presentation here today, that the bill in as far as it deals with this mandatory reporting is beneficial, and an improvement over the voluntary system of reporting that exists today. However, in going forward into the future, there should be a time that section 163 is looked at in a serious way and the issues you brought up should be raised.

It seems to me this bill is not necessarily the mechanism to address the issues you raise. It is not that broad in its scope. However, it should not be forgotten that section 163 should be reviewed in the not-too-distant future, is that not what you are suggesting?

Mr. Bernstein: That is a good reframing of the points I was trying to convey in the written submission and in the oral presentation. I am a lawyer and I should have identified that. I did consult with some law professor colleagues of mine in terms of obtaining their perspective. I think both of them felt that section 163.1 required some amendment in terms of bringing it up to date and looking at some of these other activities that could inadvertently catch young people.

I certainly did not want to come here and suggest to this committee that you should not proceed with passing Bill C-22 until we re-examine section 163.1. I do not think that is practical. The important thing is to try to address this particular mischief at play and to enact a piece of legislation that will require mandatory reporting.

I was chief counsel to a Children's Aid Society for 20 years in Toronto, and I know how valuable it is in terms of having mandatory reporting, enhancing public awareness, and having people conscious that they have a public responsibility to protect children. We need to put in place this safety net for children and young people.

I am concerned that it is precisely some of those young people in the youth criminal justice system and in the child protection system who could be caught unawares and who could inadvertently be charged. Some of this could be addressed through police charging guidelines and prosecutorial guidelines. I do think it is important to identify the need at some future date to re-examine section 163.1 so that it can work in lockstep with and support the purposes of Bill C-22.

Senator Wallace: Mr. Gillespie, I think this is stating the obvious, having listened to what you have told us. There is no question in your mind that the focus of Bill C-22, being to take reporting from a voluntary mechanism to mandatory, is the way to go, that it will be a definite improvement over what exists today?

Mr. Gillespie: Absolutely.

fournisseurs de services Internet de signaler les cas portés à leur attention. C'est dire qu'il n'est pas question ici de remanier l'article 163 du Code criminel du Canada, où sont définis les éléments constitutifs de la pornographie juvénile.

Compte tenu des arguments que vous avez avancés aujourd'hui, il me semble juste de dire que ce projet de loi, qui prévoit la déclaration obligatoire, constitue un progrès, une amélioration par rapport à l'actuelle déclaration facultative. Cela dit, il conviendrait par la suite de se pencher très sérieusement sur l'article 163 ainsi que sur les questions que vous avez soulevées aujourd'hui.

D'après moi, ce projet de loi ne répond pas nécessairement aux questions que vous avez soulevées. Sa portée est trop restreinte pour cela. Il convient, cela dit, de ne pas perdre de vue que l'article 163 devra être révisé à assez brève échéance. N'est-ce pas ce que vous prônez?

M. Bernstein : C'est, je crois, un bon résumé des idées que je souhaitais exposer à la fois dans mon mémoire écrit et dans mon exposé oral. Je suis avocat et peut-être aurais-je dû le préciser. J'ai à cet égard consulté des collègues professeurs de droit afin de recueillir leur avis. Ils estiment tous deux que l'article 163.1 devrait être modifié afin de le moderniser pour prendre en compte certaines de ces autres activités dans lesquelles des jeunes pourraient être impliqués.

Je ne voulais pas sous-entendre que le comité ne devrait pas se prononcer en faveur du projet de loi C-22 avant la refonte de l'article 163.1. Une telle solution ne serait pas pratique. L'important est de faire quelque chose pour lutter contre cette sinistre activité et adopter ce texte qui impose la déclaration obligatoire.

J'ai été, pendant 20 ans à Toronto, avocat principal de la Société d'aide à l'enfance et je sais combien il est important de rendre cette déclaration obligatoire, de sensibiliser le public, et de faire comprendre que la protection des enfants est une responsabilité que nous partageons tous. Il est donc essentiel de renforcer, à l'intention des enfants et des adolescents, le dispositif de sécurité.

Je m'inquiète à l'idée que ce pourrait être justement ces jeunes qui ont maille à partir avec la justice pénale des jeunes, et avec le système de protection de l'enfance, qui risquent le plus de se voir accuser de choses qu'ils ont faites plutôt par inconscience. Une partie du problème pourrait être réglée par la rédaction, tant à l'intention de la police que des procureurs, de lignes directrices en matière d'accusations. Il est d'après moi important de prévoir dès maintenant qu'il va falloir revoir l'article 163.1 afin de le mettre en harmonie avec les objectifs du projet de loi C-22.

Le sénateur Wallace : Ne peut-on pas dire, monsieur Gillespie, qu'il ne fait, selon vous, aucun doute que l'adoption de ce projet de loi, qui rend obligatoire la déclaration qui jusqu'ici n'était que facultative, est un réel progrès par rapport à la situation actuelle?

M. Gillespie : Tout à fait.

Senator Wallace: As Mr. Bernstein has said — and I think you made much the same comment — this is an important step, but there are other steps that, as a government, we should be moving forward with a review of section 163.1 perhaps being appropriate?

Mr. Gillespie: Certainly.

[Translation]

Senator Carignan: My question is for Mr. Bernstein. I am a bit surprised at the emphasis you place, in the brief you have presented to us, on the problem with section 163.1 of the Criminal Code. The purpose of Bill C-22 is to protect children, to make Internet service providers accountable and to create a system of exchange of information to provide the best protection for children. Through the presentation that you made to us in your brief, and it is as though you were saying that we have to watch out because, by reporting, we may harm children because innocent children could be charged with accessing child pornography material because children will, innocently perhaps, be inclined to exchange information or — somewhat as for the Supreme Court judgment and the exception in the *Sharpe* affair — will be led involuntarily to commit offences. It is as though we were forgetting the main point and focusing solely on a minor exception. I believe you are placing disproportionate emphasis on the problem of children who might be prosecuted.

First, to your knowledge, under section 163.1, have a lot of charges been laid against children in this connection? I am really surprised that so much emphasis has been placed on this.

Second, do you not believe that the mechanism created in clause 2 of Bill C-22, with a designated organization, does indeed protect children? That mechanism provides, for example, that, if the designated organization is called the Canadian Centre for the Protection of Children, technicians, specialized analysts, will analyze the information before forwarding it to police officers. Do you not think this mechanism is a balanced measure of extraordinary law to protect children and to distinguish between an innocent, technical offence committed by a child and offences committed by actual pedophiles, who are the ones we aim to arrest?

[English]

The Chair: Do you have the general sense of that question?

Mr. Bernstein: Yes, I do.

As I said, having been involved in the field of child protection in Ontario for 28 years before I went out to the province of Saskatchewan, and in my role as a provincial children's advocate, I saw many young people victimized, who came and brought their concerns to my office. Child sexual exploitation often happened in tragic circumstances, and sometimes to very vulnerable and marginalized child populations. That clearly is an important

Le sénateur Wallace : M. Bernstein a dit — et je crois que vous vous êtes prononcé dans le même sens — qu'il s'agit d'une étape importante, mais que le gouvernement devrait en outre remanier l'article 163.1.

M. Gillespie : En effet.

[Français]

Le sénateur Carignan : Ma question s'adresse à M. Bernstein. Je suis un peu surpris de l'accent que vous mettez, dans le mémoire que vous nous avez présenté, sur la problématique de l'article 163.1 du Code criminel. Le projet de loi C-22 vise à protéger les enfants, à responsabiliser les fournisseurs de services Internet et à créer un système d'échange d'informations, de façon à assurer une meilleure protection des enfants. De par la présentation que vous en faites dans votre mémoire, c'est comme si vous disiez qu'il faut faire attention parce qu'en dénonçant, on risque de porter atteinte aux enfants, car des enfants innocents pourraient se voir accuser d'avoir eu accès à du matériel de pornographie juvénile parce que, innocemment, peut-être, des enfants vont être portés à faire des échanges ou — un peu comme pour le jugement de la Cour suprême et l'exception dans l'affaire *Sharpe* — vont être portés involontairement à commettre des infractions. C'est comme si on oubliait le principal et on s'attachait à seulement une petite exception. Je trouve disproportionné l'accent que vous mettez sur la problématique des enfants qui pourraient se voir poursuivre.

Est-ce que, dans un premier temps, selon votre connaissance, en vertu de l'article 163.1, il y a eu beaucoup d'accusations portées contre des enfants aux termes de cette problématique? Pour mettre autant l'accent là-dessus, je suis vraiment surpris.

Deuxièmement, ne croyez-vous pas que le mécanisme créé à l'article 2 du projet de loi C-22, avec un organisme désigné, vient justement protéger les enfants? Ce mécanisme prévoit par exemple, si l'organisme désigné s'appelle le Centre canadien de la protection de l'enfance, que des techniciens, des analystes spécialisés, vont analyser l'information avant de la transmettre aux policiers. Ne trouvez-vous pas que ce mécanisme est une mesure d'équilibre du droit extraordinaire pour protéger les enfants et faire la part des choses entre une infraction innocente, technique, commise par un enfant, et des infractions commises par de vrais pédophiles, qui sont ceux qu'on vise à arrêter?

[Traduction]

La présidente : Avez-vous saisi le sens de la question?

M. Bernstein : Oui.

Comme je le disais tout à l'heure, après avoir travaillé pendant 28 ans en Ontario dans le domaine de la protection de l'enfance, avant d'exercer en Saskatchewan, les fonctions de protecteur des enfants, j'ai eu affaire à de nombreuses jeunes victimes qui ont pris contact avec mes services et fait part de leurs difficultés. L'exploitation sexuelle d'enfants s'inscrit très souvent dans le cadre de circonstances tragiques par ailleurs. Souvent, les enfants

constituency to protect. I want to be unequivocal that that is a position that I and UNICEF completely support in terms of the purposes of this bill.

We did attempt to ascertain from both Nova Scotia and Manitoba whether or not there is a tracking of prosecutions or the laying of charges against young people. In one instance, we were told that that information could not be ascertained and was not being tracked; and in the other instance, we had made several attempts and the response was not transmitted back to us. I do not have clear data. I would expect that it is infrequent, but it is a concern.

Sometimes, at least in my experience, we tend to artificially differentiate between child victims, and sometimes we stigmatize children and we create an impression that there are young people who are victimizing other children. Even in terms of the concepts and the language that we are using around this table, I am not entirely comfortable with it.

I did a report when I was in Saskatchewan on child sexual exploitation. The term that was thrown around at times was “child prostitution.” We took the position that that was not proper language, that young people do not make an occupational preference; it is exploitation.

Here the same thing; child sexual images are a form of child sexual abuse. We are talking about child pornography because that is the reference point. That is the language of the Criminal Code.

Certainly, in terms of the primary emphasis of this bill, I could not agree more with you that it is an important piece of legislation. I am just saying let us not forget that there may be a smaller group of young people who could run afoul of this because they are not aware of the implications, they do not understand the legislation in terms of the Criminal Code, and they have not received any preventive education. Let us try to work together to put all those pieces together. I think that is what I am trying to emphasize tonight.

[Translation]

Senator Carignan: I do not believe you entirely answered the last part of my question, which concerned the role of the Canadian Centre for the Protection of Children as the designated organization and the fact that it strikes a good balance for the purpose of preventing the negative impact that you mention in your brief.

[English]

Mr. Bernstein: Just briefly on that point, I think it could be an effective filter in terms of receiving the information and determining that this seems to be more of an innocent exchange

sont issus de populations marginalisées et particulièrement vulnérables. Il s'agit d'un groupe qu'il est spécialement important de protéger. C'est pourquoi je tiens à dire, sans la moindre ambiguïté, que l'UNICEF est entièrement acquis aux objectifs de ce projet de loi.

Nous avons contacté les services compétents en Nouvelle-Écosse et au Manitoba afin de savoir s'ils avaient mis en place un mécanisme permettant de comptabiliser à part les poursuites ou les accusations portées contre des jeunes. Les uns nous ont répondu que ce renseignement n'était pas disponible et que les dossiers en question n'étaient pas comptabilisés à part, et les autres ne nous ont pas répondu, malgré plusieurs efforts faits pour les relancer. Je n'ai donc, sur ce point, aucun renseignement particulier, j'imagine que cela ne se produit que rarement, mais c'est tout de même quelque chose dont on doit se préoccuper.

Il m'est arrivé de constater que, parfois, les gens font une distinction entre les diverses jeunes victimes, distinction qui entraîne une stigmatisation de certains enfants et donne l'impression que leur victimisation est parfois le fait d'autres enfants. Les concepts et les termes que nous employons ici me mettent un peu mal à l'aise.

Lorsque j'étais en poste en Saskatchewan, j'ai rédigé un rapport sur l'exploitation sexuelle des enfants. À l'époque, on parlait parfois de « prostitution infantine ». Nous avons fait valoir que ce n'était pas un terme à employer, étant donné que les enfants en question n'optent guère pour ce métier; il s'agit d'exploitation pure et simple.

J'estime qu'il en va de même en l'occurrence; les images sexuellement explicites d'enfants, constituent une exploitation sexuelle des enfants. Si nous employons le terme pornographie juvénile, c'est parce que le terme est employé par le Code criminel.

En ce qui concerne la principale disposition du projet de loi, je suis entièrement d'accord avec vous quant à son importance. Je tiens simplement à insister sur le fait qu'il ne nous faut pas perdre de vue que certains jeunes risquent d'en subir les conséquences étant donné qu'ils ne comprennent pas ce qui est inscrit au Code criminel, et qu'ils n'ont, en ce domaine, bénéficié d'aucune éducation préventive. Tentons donc de travailler de concert afin de mettre en cohérence tous ces divers éléments. C'est sur cela que je tiens à insister ce soir.

[Français]

Le sénateur Carignan : Je pense que vous n'avez pas tout à fait répondu à la dernière partie de ma question, qui portait sur le rôle que joue le Centre canadien de la protection de l'enfance comme organisme désigné et le fait qu'il apporte un bel équilibre pour, justement, éviter les impacts négatifs dont vous avez fait mention dans votre mémoire.

[Traduction]

M. Bernstein : Pour revenir, très rapidement, à la question, je pense que cela pourrait être un moyen de filtrage efficace permettant de distinguer les échanges innocents entre deux

between two curious young people, and not to refer that on to the police for purposes of laying the charge. That could be an added safeguard in terms of responding to your question.

The Chair: Did you want to add anything, Mr. Gillespie?

Mr. Gillespie: No.

Senator Angus: Thank you, gentlemen.

Mr. Gillespie, I was impressed with your experience in these things and your technological expertise. You were present here and saw us technically challenged liberal-arts graduates wrestling with the testimony of the previous witness.

Did you understand the point he was trying to make and do you agree with what he said?

Mr. Gillespie: First, when I started in this section, I had a hard time sending an email or knowing whether I had saved a file properly. My generation did not grow up with the technology, so I am learning, and it is very difficult, not like it is for our children and grandchildren.

I got the gist of what he said. As with anything new, it is easy to be overwhelmed. Experts can wow with ideas or philosophies that are really hard to pare down to basic language that the layman might understand.

The only point I really agreed with him on was his last point, that being that the technical ability exists to stop this. Everything he said up to that point was his view, I believe. I am not sure if I agree with him, and I reached a conclusion similar to that which many of you probably arrived at.

Senator Angus: The gist of the bill is to render mandatory what is presently voluntary, namely, that the ISPs will now be under pain of penalty if they do not report. He is sort of an ISP. Is it feasible that he was making the point to avoid extra work, or is that being a little paranoid?

Mr. Gillespie: I have been around the world of ISPs for many years and watched this issue evolve. He could have all sorts of motives for saying what he did. I do not know because I do not know the man or what he does for a living.

However, I think that he interprets, by definition, networks, computers and infrastructure in a way that would back up his argument, and it simply might be interpreted differently by other people. I think we would all agree that there is a moral obligation. It is, however, imperative that there be a legal obligation as well so

jeunes personnes qui manifestent une curiosité naturelle, et ne pas les signaler par conséquent à la police. Je crois que cela pourrait offrir une garantie supplémentaire.

La présidente : Avez-vous quelque chose à ajouter, monsieur Gillespie?

M. Gillespie : Non.

Le sénateur Angus : Merci, messieurs.

Monsieur Gillespie, vous nous avez fait part d'une expérience et de connaissances technologiques tout à fait impressionnantes. Vous avez pu constater les difficultés que ceux qui ont fait des études d'arts et lettres éprouvent à l'égard de questions techniques telles que celles qu'a évoquées notre témoin précédent.

Avez-vous saisi pleinement le sens de son intervention, et êtes-vous d'accord avec ce qu'il nous a dit?

M. Gillespie : Au départ, j'avais du mal ne serait-ce qu'à envoyer un courriel ou à savoir si j'avais correctement sauvegardé un fichier. La génération dont je fais partie n'a pas grandi avec toute cette technologie et je continue donc à apprendre et c'est parfois difficile alors que cela paraît simple à nos enfants et à nos petits enfants.

J'ai saisi en gros le sens de son propos. On peut facilement se sentir dépassé par ce qui est nouveau. Les experts peuvent vraiment nous impressionner avec des idées ou des concepts qu'ils ont du mal à exprimer plus simplement afin de se mettre à la portée des profanes.

Le seul point sur lequel je sois entièrement d'accord avec lui est lorsqu'il a dit, pour finir, que les moyens techniques de mettre fin à cela existent déjà. Jusque-là, il exprimait simplement son point de vue sur divers aspects de la question. Je ne suis pas certain d'être d'accord avec lui et je suis parvenu à une conclusion qui n'est sans doute pas très éloignée de celle à laquelle ont abouti bon nombre d'entre vous.

Le sénateur Angus : Le but essentiel de ce projet de loi est de rendre obligatoire ce qui n'était jusqu'ici que facultatif, c'est-à-dire d'imposer aux FSI, sous peine de sanctions, l'obligation de déclarer. Or, il est lui-même, en quelque sorte, un FSI. Est-ce à dire qu'il cherchait surtout à s'éviter une tâche supplémentaire, ou qu'il s'inquiète exagérément?

M. Gillespie : Je fréquente depuis de nombreuses années le milieu des FSI et j'ai pu constater comment la question a évolué. Il pouvait avoir toutes sortes de raisons de dire ce qu'il a dit. Je n'ai aucun moyen de les connaître étant donné que je ne connais pas l'homme, et que je ne sais pas en quoi consistent ses activités professionnelles.

Sa conception des réseaux, des ordinateurs et de l'infrastructure sert de fondement à son argumentation et d'autres pourraient très bien en donner une interprétation différente. Nous sommes tous, je pense, d'accord qu'il existe à cet égard une obligation morale. Cela dit, il faut que celle-ci s'accompagne d'une obligation juridique afin

that people do not have the choice. If you find a loaded gun or a bag of cocaine, you call the police. Why is it any different with this?

The Chair: Mr. Gillespie, you said that for now this bill is worthwhile and important, but that down the road, and I got the impression that you meant not that far down the road, there will not be enough human bodies to do the work necessary to control this and that we will need technological means of some sort.

Will you expand on that a bit? Are you talking about something like clean feed that blocks transmission or are you talking about more advanced technology so that robots, if you will, will cruise the Internet and find out who is responsible for things rather than us only blocking transmission?

Mr. Gillespie: That is a great question and you described exactly what can happen now. In *Star Wars*, every time robots saw a horrible picture, they could shoot it and destroy it. That is available now.

Clean feed is simply an opportunity to block access to bad websites. In my opinion, the vast majority of these horrible pictures are not from websites. They may be sometimes but that is a very small percentage. Predators share their files today through file-sharing programs in the same way that Napster started so that we could share music without having to pay royalties. It is now illegal to do that in the United States, although it is still legal in Canada.

Pedophiles and predators use the exact same technology to share these horrible pictures. Global police are in possession of hundreds of thousands of Internet protocol addresses of people who share these pictures every day, and many of them are in Canada.

Police also have the ability to watch these pictures flying through the Internet. They can tell exactly where they came from and they know which pictures they are. Again, hundreds of thousands of people are sharing these horrible pictures of prepubescent, typically five- and six-year-old, victims of horrific abuse.

People have opinions. In my opinion, there are about 1 million original images of child abuse on the Internet. Some people say there are as many as 5 million. I believe that about 50,000 different kids are involved, and through the best efforts of global law enforcement, we have identified less than 2,000 of these kids.

The only science we have with regard to people who collect and share pictures is that about 35 per cent to 40 per cent are believed to be actual hands-on abusers. If you are going to collect and trade child pornography, there is a three- to four-out-of-ten chance that you are an abuser. If I told you that in Canada there

que la chose ne soit pas simplement facultative. Si vous trouvez un revolver chargé, ou un sac plein de cocaïne, vous appelez la police. Je ne vois pas pourquoi il irait autrement en l'occurrence.

La présidente : Monsieur Gillespie, vous nous avez dit que ce projet de loi mérite d'être adopté, qu'il est important, mais que, si je vous ai bien compris, les ressources humaines vont bientôt nous manquer pour assurer les contrôles nécessaires et nous allons donc devoir trouver des moyens techniques d'effectuer ce travail.

Pourriez-vous nous en dire un peu plus à cet égard? Entendez-vous par cela quelque chose comme le système « clean feed » qui bloque les transmissions, ou des technologies plus avancées encore telles que des robots qui pourraient naviguer sur Internet et repérer les responsables au lieu de simplement bloquer leurs transmissions?

M. Gillespie : C'est effectivement la question et vous venez de décrire des moyens qui existent déjà. Dans le film *Star Wars*, à chaque fois qu'un robot se trouvait face à une image atroce, il la détruisait. Ces moyens existent déjà.

Le système clean feed permet de bloquer l'accès aux sites Internet malfaisants. Je pense, cependant, que l'immense majorité de ces images atroces ne proviennent pas de sites Internet. Parfois oui, mais seulement pour un très faible pourcentage. Les prédateurs se transmettent cela au moyen de programmes de partage de fichiers. C'est un peu le même système que Napster, qui permettait aux gens de s'échanger de la musique sans avoir à verser de redevances. Ce système est devenu illégal aux États-Unis, bien qu'il ne le soit pas encore au Canada.

Les pédophiles et les prédateurs ont recours à cette même technologie pour diffuser ces images atroces. Les policiers des divers pays ont, dans leurs fichiers, des centaines de milliers d'adresses Internet de personnes qui chaque jour se transmettent ce genre d'images, dont bon nombre se trouvent d'ailleurs au Canada.

La police a actuellement les moyens de capter cette transmission d'images par Internet. Elle est en mesure d'en connaître la source et le contenu. Il y a, je le dis bien, des centaines de milliers de personnes qui se transmettent ces images atroces d'enfants, âgés généralement de cinq à six ans, victimes d'effroyables sévices.

Chacun peut se faire une idée de l'ampleur du phénomène. Selon moi, Internet recèle actuellement environ un million d'images originales de sévices à l'enfant. Certains diront qu'il y en a cinq millions. D'après moi, 50 000 enfants sont actuellement impliqués dans cet atroce trafic, et toutes les polices du monde ne sont jusqu'ici parvenues qu'à en identifier moins de 2 000.

Les seuls renseignements vraiment fiables que nous ayons au sujet des gens qui collectionnent et diffusent ce genre d'images indiquent qu'entre 35 et 40 p. 100 d'entre eux seraient eux-mêmes auteurs de ces brutalités. Il y a donc trois ou quatre chances sur 10 pour que ceux qui collectionnent et diffusent de la pornographie

are tens of thousands of Canadian IPs trading this terrible filth daily, and you assume that 30 per cent to 40 per cent are hands-on abusers, you can do the math for yourself.

This is a bucket that is overflowing for law enforcement. I think that human eyes will never get back what technology has exploited and manifested in an exponential way that no one envisioned.

I am not trying to be alarmist, but I would invite you to ask law enforcement to explain exactly what the numbers are so that people can have a better understanding of what the challenges are. I am not sure that society is really informed on this, and maybe they do not want to know, but it is pretty bad.

The Chair: It is certain that many people do not want to think about it, and that is why senators, and people like you even more so, get tasked with this.

I believe you are saying that some technology is available now but that more is needed, that we could not do now what we need to do.

Mr. Gillespie: We could not in a million years investigate all of the tips following legal process. We do, however, have the technical ability to get rid of these millions and millions of pictures that are being traded each day.

Senator Angus: That exists now?

Mr. Gillespie: Yes, and that is what Mr. MacKay was alluding to, although all the issues that that brings up would have to be dealt with.

The Chair: My question was how long it will be before we have the kind of technology you are talking about, and the answer is that some of it is available now.

Mr. Gillespie: Absolutely.

The Chair: Gentlemen, thank you very much. This has been fascinating, and we are very grateful to both of you.

(The committee adjourned.)

OTTAWA, Thursday, February 17, 2011

The Standing Senate Committee on Legal and Constitutional Affairs, to which was referred Bill C-22, An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service, met this day at 10:37 a.m. to give clause-by-clause consideration to the bill.

Senator Joan Fraser (*Chair*) in the chair.

juvénile soient eux-mêmes auteurs de ce genre de sévices. Vous pouvez faire vous-mêmes le calcul, étant donné qu'il y a au Canada des dizaines de milliers d'adresses IP qui s'échangent chaque jour ces images immondes et que de 30 à 40 p. 100 des individus concernés sont eux-mêmes auteurs de tels sévices.

Les organismes répressifs sont débordés. Je pense que nous ne parviendrons pas par nos seuls moyens humains à saisir à nouveau le contrôle de cette technologie actuellement exploitée d'une manière que personne n'avait envisagée.

Je ne voudrais pas passer pour un alarmiste, mais je vous invite à demander aux responsables policiers de vous expliquer l'ampleur du phénomène afin que chacun saisisse bien l'importance du problème. Je ne suis pas sûr que les gens soient, en général, vraiment conscients de ce qui se passe, et peut-être ne veulent-ils pas le savoir, mais la situation est grave.

La présidente : Il est clair que beaucoup de gens ne souhaitent même pas y penser, et c'est pour cela que les sénateurs, et encore plus les gens qui, comme vous, se consacrent à ce problème, doivent y réfléchir.

Vous avez dit, je crois, que certains moyens technologiques existent déjà, mais qu'il nous faut en trouver d'autres, car nous n'avons pas actuellement les moyens d'agir comme nous devrions le faire.

M. Gillespie : Il nous serait absolument impossible d'enquêter sur tous les indices qui nous sont transmis. Il nous serait, cependant, techniquement possible de supprimer ces millions d'images qui, chaque jour, s'échangent.

Le sénateur Angus : Ces moyens existent actuellement?

M. Gillespie : Oui, et c'est de cela que voulait parler M. MacKay même si, bien sûr, il faudra en même temps régler les questions que cela pourrait soulever par ailleurs.

La présidente : J'allais vous demander combien de temps il nous faudrait pour mettre en œuvre les moyens techniques que vous venez d'évoquer, mais, selon vous, ces moyens existent déjà.

M. Gillespie : Tout à fait.

La présidente : Merci, messieurs. Nous vous sommes reconnaissants de tous ces éléments d'information que vous nous avez livrés.

(La séance est levée.)

OTTAWA, le jeudi 17 février 2011

Le Comité sénatorial permanent des affaires juridiques et constitutionnelles, auquel a été renvoyé le projet de loi C-22, Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet, se réunit aujourd'hui à 10 h 37 pour procéder à l'étude article par article de ce projet de loi.

Le sénateur Joan Fraser (*présidente*) occupe le fauteuil.

[English]

The Chair: Honourable senators, welcome. As you know, the agenda today consists of clause-by-clause consideration of Bill C-22, An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service.

We have heard a number of witnesses on this bill. However, before I ask you to proceed to clause-by-clause, there is one last submission that I will read into the record so that all colleagues have the benefit of it. This is a submission that came in this morning from Mr. Michael MacKay, the expert witness who appeared before us last night. In this context, I am sure you will join with me in thanking the interpreters for what has to be an even more complicated than usual task of translating some of the technical jargon that we have heard.

Mr. MacKay has written to us as follows:

During my appearance before the Committee on 16 February 2011, I was asked what was wrong with making ISPs have a special requirement to report IP addresses and URLs. The short answer is there is nothing wrong with that but that we can go much further and, in the process, make the matter simpler. The provinces of Manitoba and Nova Scotia already have legislation in place and Alberta has a bill on this subject, all with wording similar to this: "Any person who has reasonable and probable grounds to believe that a representation or material is child pornography shall immediately report the matter to a reporting entity." This language frees us from trying to determine who is an ISP and it speeds up the process. Since law enforcement is going to have to process the information anyways, we should try to get the data (the child pornography image) and metadata (the IP address and the URL) to them right away instead of going through an ISP (if you can figure out who the ISP is, that is).

I have also tried to dispel the notion that ISPs have a special or privileged knowledge that is not available to all users of the Internet. The Internet is more of a conversation between equals than it is users being told what to do by ISPs. While not every user of the Internet has great technical knowledge, this is not necessary for fulfilling every citizen's duty to report the instances of child pornography when they come across them."

That is the submission from Mr. MacKay.

[Traduction]

La présidente : Chers collègues, bonjour. Comme vous le savez, nous devons procéder aujourd'hui à l'étude article par article du projet de loi C-22, Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet.

Nous avons entendu plusieurs témoins dans le cadre de notre étude de ce projet de loi. Avant de vous demander d'entreprendre l'étude article par article, j'aimerais toutefois vous faire lecture aux fins du compte rendu d'une dernière lettre que l'on nous a envoyée, de telle sorte que tous les membres du comité puissent en bénéficier. Nous l'avons reçue ce matin de M. Michael MacKay, le témoin expert qui a comparu devant nous hier soir. Dans ce contexte, je suis persuadée que vous joindrez vos voix à la mienne pour remercier nos interprètes qui ont dû accomplir un travail encore plus compliqué qu'à l'habitude pour traduire le jargon technique auquel nous avons parfois eu droit.

Voici donc ce que nous écrit M. MacKay :

Pendant ma comparution devant le comité, le 16 février 2011, on m'a demandé en quoi le fait que les fournisseurs de services Internet aient l'obligation particulière de déclarer les adresses IP et les URL posait problème. Je peux uniquement dire qu'il n'y a rien de mal à cela, mais que nous pouvons aller beaucoup plus loin et, par la même occasion, faire les choses plus simplement. Les provinces du Manitoba et de la Nouvelle-Écosse ont déjà adopté des mesures législatives dans ce sens, et l'Alberta a présenté un projet de loi sur ce sujet, lesquels ont tous des libellés semblables à ceci : « Quiconque a des motifs raisonnables et probables de croire qu'une représentation ou un document constitue de la pornographie juvénile doit immédiatement en informer l'entité chargée de traiter les signalements. » Ce libellé nous libère de l'obligation de nous efforcer de déterminer qui est le fournisseur d'accès Internet et accélère le processus. Étant donné que les forces de l'ordre devront traiter les renseignements de toute façon, nous devrions tenter de leur envoyer les données (l'image de pornographie juvénile) et les métadonnées (l'adresse IP et l'URL) sans délai, au lieu de passer par un fournisseur de services Internet (c'est-à-dire si l'on peut deviner qui est le fournisseur de services Internet).

Je tente aussi de dissiper l'idée que les fournisseurs de services Internet ont des connaissances particulières ou privilégiées qui ne sont pas accessibles à tous les internautes. Internet est plutôt une conversation entre égaux que des utilisateurs qui se font dire quoi faire par des fournisseurs de services Internet. Les utilisateurs d'Internet n'ont pas tous de grandes connaissances techniques, mais cela n'est pas nécessaire pour remplir son devoir de citoyen et signaler les cas de pornographie juvénile lorsqu'on tombe sur de tels cas.

C'était la lettre de M. MacKay.

We have just received a submission from Facebook, from someone who had been received before the committee as a witness. This is very late in the day, colleagues. It is a short, one-page, three-paragraph submission. Do you wish to wait until we can have that printed out and see it, or are you willing to proceed on the basis of what we have already heard? I am in your hands.

Senator Angus: Proceed.

Some Hon. Senators: Yes.

The Chair: We will, of course, circulate the submission from Facebook.

Senator Joyal: Can we have it printed?

The Chair: We shall have it printed.

Senator Munson: It is too bad it was not Twitter.

The Chair: Should it contain material that affects our view of the bill, there is, of course, always the third-reading phase at which that can be addressed.

Finally, honourable senators, I would ask you all to use, as you consider this bill, the version passed by the House of Commons on December 3 because, as we know, there has been more than one version of this bill.

[*Translation*]

Is it agreed that the committee proceed to clause-by-clause consideration of Bill C-22, An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service?

Hon. Senators: Yes.

The Chair: Is everyone in agreement? Carried.

[*English*]

Shall the title stand postponed? Agreed?

Hon. Senators: Agreed.

The Chair: Opposed? Abstentions? Carried.

Shall clause 1 carry?

Hon. Senators: Agreed.

The Chair: Carried.

[*Translation*]

Shall clause 2 carry?

Hon. Senators: Agreed.

The Chair: Carried.

[*English*]

Shall clause 3 carry?

Nous venons tout juste également de recevoir un message de Facebook qui nous est transmis par le représentant qui a comparu comme témoin devant notre comité. C'est vraiment ce qu'on appelle à la dernière minute, chers collègues. C'est un bref message de trois paragraphes. Souhaitez-vous que nous attendions que ce message ait été imprimé pour que tous puissent en prendre connaissance, ou êtes-vous disposés à poursuivre sur la foi de ce que nous avons déjà entendu? C'est à vous de décider.

Le sénateur Angus : Poursuivons.

Des voix : Oui.

La présidente : Nous allons bien sûr vous distribuer le message reçu de Facebook.

Le sénateur Joyal : Peut-on le faire imprimer?

La présidente : C'est ce que nous ferons.

Le sénateur Munson : C'est dommage qu'ils n'aient pas utilisé Twitter.

La présidente : Si l'on devait y trouver des éléments susceptibles d'influer sur notre opinion au sujet du projet de loi, on pourra toujours, bien sûr, faire le nécessaire à l'étape de la troisième lecture.

Enfin, je vous rappelle à tous que nous devons utiliser pour l'étude de ce projet de loi la version adoptée par la Chambre des communes le 3 décembre dernier car, comme nous le savons tous, ce projet de loi n'en est plus à sa première mouture.

[*Français*]

Est-il convenu de procéder à l'étude article par article du projet de loi C-22, Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet?

Des voix : Oui.

La présidente : Tout le monde est d'accord? Adopté.

[*Traduction*]

Êtes-vous d'accord pour suspendre l'adoption du titre?

Des voix : D'accord.

La présidente : Ceux qui sont contre? Des abstentions? Adopté.

L'article 1 est-il adopté?

Des voix : D'accord.

La présidente : Adopté.

[*Français*]

L'article 2 est-il adopté?

Des voix : D'accord.

La présidente : Adopté.

[*Traduction*]

L'article 3 est-il adopté?

Hon. Senators: Agreed.

The Chair: Carried.

[*Translation*]

Shall clause 4 carry?

[*English*]

Hon. Senators: Agreed.

The Chair: Carried, on division.

Shall clause 5 carry?

Hon. Senators: Agreed.

The Chair: Agreed.

Shall clause 6 carry?

Senator Joyal: On division.

The Chair: Clause 6 is carried, on division.

[*Translation*]

Shall clause 7 carry?

Hon. Senators: Agreed.

The Chair: Carried.

Shall clause 8 carry?

Hon. Senators: Agreed.

The Chair: Carried.

[*English*]

Shall clause 9 carry?

Hon. Senators: Agreed.

The Chair: Carried.

Shall clause 10 carry?

Hon. Senators: Agreed.

The Chair: Carried.

[*Translation*]

Shall clause 11 carry?

Hon. Senators: Agreed.

The Chair: Carried.

Shall clause 12 carry?

Hon. Senators: Agreed.

The Chair: Carried.

[*English*]

Shall clause 13 carry?

Hon. Senators: Agreed.

The Chair: Carried.

Des voix : D'accord.

La présidente : Adopté.

[*Français*]

L'article 4 est-il adopté?

[*Traduction*]

Des voix : D'accord.

La présidente : Adopté, avec dissidence.

L'article 5 est-il adopté?

Des voix : D'accord.

La présidente : Adopté.

L'article 6 est-il adopté?

Le sénateur Joyal : Avec dissidence.

La présidente : L'article 6 est adopté, avec dissidence.

[*Français*]

L'article 7 est-il adopté?

Des voix : D'accord.

La présidente : Adopté.

L'article 8 est-il adopté?

Des voix : D'accord.

La présidente : Adopté.

[*Traduction*]

L'article 9 est-il adopté?

Des voix : D'accord.

La présidente : Adopté.

L'article 10 est-il adopté?

Des voix : D'accord.

La présidente : Adopté.

[*Français*]

L'article 11 est-il adopté?

Des voix : D'accord.

La présidente : Adopté.

L'article 12 est-il adopté?

Des voix : D'accord.

La présidente : Adopté.

[*Traduction*]

L'article 13 est-il adopté?

Des voix : D'accord.

La présidente : Adopté.

Shall the title carry?

Hon. Senators: Agreed.

The Chair: Carried.

[*Translation*]

Shall the bill carry?

Hon. Senators: Yes.

Hon. Senators: On division.

The Chair: Carried on division.

[*English*]

Does the committee wish to append observations to the report?

Senator Wallace: Yes, I have a comment on that.

The Chair: Senator Wallace, normally we would go in camera to discuss observations. Do you wish us to discuss observations?

Senator Wallace: We could do that in camera, thank you.

The Chair: Is it agreed?

Hon. Senators: Agreed.

The Chair: We will ask non-staff of members of this committee to please leave this room.

(The committee continued in camera).

Le titre est-il adopté?

Des voix : D'accord.

La présidente : Adopté.

[*Français*]

Le projet de loi est-il adopté?

Des voix : Oui.

Des voix : Avec dissidence.

La présidente : Adopté avec dissidence.

[*Traduction*]

Est-ce que le comité veut annexer des observations au rapport?

Le sénateur Wallace : Oui, j'ai un commentaire à ce sujet.

La présidente : Sénateur Wallace, normalement nous devrions poursuivre à huis clos pour discuter des observations. Est-ce que c'est ce que vous souhaitez faire?

Le sénateur Wallace : Nous pourrions le faire à huis clos.

La présidente : Vous êtes d'accord?

Des voix : D'accord.

La présidente : Nous demandons à tous ceux qui ne font pas partie du personnel ou du comité de bien vouloir quitter la salle.

(Le comité poursuit ses travaux à huis clos).

WITNESSES

Wednesday, February 16, 2011

Office of the Privacy Commissioner of Canada:

Chantal Bernier, Assistant Privacy Commissioner;

Anna Zubrzycka, Policy Analyst, Legal Services, Policy and Parliamentary Affairs Branch.

Canadian Centre for Child Protection:

Lianna McDonald, Executive Director;

Signy Arnason, Director, Cybertip.ca.

Ontario Provincial Police:

Inspector Scott Naylor, Child Sexual Exploitation Section.

Canadian Association of Chiefs of Police:

Vincent Westwick, General Counsel.

ExitCertified:

Michael MacKay, Senior Consultant.

UNICEF Canada:

Marvin Bernstein, Chief Advisor, Advocacy.

Kids Internet Safety Alliance:

Paul Gillespie, President and Chief Executive Officer.

TÉMOINS

Le mercredi 16 février 2011

Commissariat à la protection de la vie privée du Canada :

Chantal Bernier, commissaire adjointe à la protection de la vie privée;

Anna Zubrzycka, analyste politique, Direction des services juridiques, des politiques et des affaires parlementaires.

Centre canadien de protection de l'enfance :

Lianna McDonald, directrice générale;

Signy Arnason, directrice, Cyberaide.ca.

Police provinciale de l'Ontario :

Inspecteur Scott Naylor, Unité de la pornographie juvénile.

Association canadienne des chefs de police :

Vincent Westwick, avocat général.

ExitCertified :

Michael MacKay, consultant principal.

UNICEF Canada :

Marvin Bernstein, conseiller principal, Promotion et défense des droits.

Kids Internet Safety Alliance :

Paul Gillespie, président-directeur general.