Third Session
Thirty-seventh Parliament, 2004

SENATE OF CANADA

Proceedings of the Standing Senate Committee on

Transport and Communications

Chair:
The Honourable JOAN FRASER

Thursday, May 6, 2004

Issue No. 10

Second meeting on:

Bill S-2, An Act to prevent unsolicited messages on the Internet

WITNESSES:
(*See back cover*)

Troisième session de la
trente-septième législature, 2004

SÉNAT DU CANADA

Délibérations du Comité sénatorial permanent des

Transports et des communications

Présidente:
L'honorable JOAN FRASER

Le jeudi 6 mai 2004

Fascicule n^{o} 10

Deuxième réunion concernant:

Le projet de loi S-2, Loi visant à empêcher la diffusion sur l'Internet de messages non sollicités

TÉMOINS:
(*Voir à l'endos*)

THE STANDING SENATE COMMITTEE ON TRANSPORT AND COMMUNICATIONS

The Honourable Joan Fraser, *Chair*

The Honourable Leonard J. Gustafson, *Deputy Chair*

and

The Honourable Senators:

Adams
* Austin, P.C.
(or Rompkey, P.C.)
Corbin
Day
Eyton
Johnson
Graham, P.C.
LaPierre
* Lynch-Staunton
(or Kinsella)
Merchant
Phalen
Spivak

* *Ex Officio Members*

(Quorum 4)

LE COMITÉ SÉNATORIAL PERMANENT DES TRANSPORTS ET DES COMMUNICATIONS

Présidente: L'honorable Joan Fraser

Vice-président: L'honorable Leonard J. Gustafson

et

Les honorables sénateurs:

Adams
* Austin, c.p.
(ou Rompkey, c.p.)
Corbin
Day
Eyton
Johnson
Graham, c.p.
LaPierre
* Lynch-Staunton
(ou Kinsella)
Merchant
Phalen
Spivak

* *Membres d'office*

(Quorum 4)

Published by the Senate of Canada

Available from: Public Works and Government Services Canada
Publishing and Depository Services, Ottawa, Ontario K1A 0S5

Also available on the Internet: http://www.parl.gc.ca

Publié par le Sénat du Canada

Disponible auprès des: Travaux publics et Services gouvernementaux Canada –
Les Éditions et Services de dépôt, Ottawa (Ontario) K1A 0S5

Aussi disponible sur internet: http://www.parl.gc.ca

MINUTES OF PROCEEDINGS

OTTAWA, Thursday, May 6, 2004
(16)

[*English*]

The Standing Senate Committee on Transport and Communications met this day at 10:55 a.m., in room 705, Victoria Building, the Chair, the Honourable Joan Fraser, presiding.

Members of the committee present: The Honourable Senators Corbin, Day, Fraser, Graham, P.C., LaPierre, Merchant, and Phalen (7).

In attendance: Terrance Thomas, Research Analyst, Parliamentary Research Branch, Library of Parliament.

Also in attendance: The official reporters of the Senate.

Pursuant to the Order of Reference adopted by the Senate on Tuesday, March 23, 2004, the committee continued its consideration of Bill S-2, to prevent unsolicited messages on the Internet.

WITNESSES:

From the Canadian Association of Internet Providers:

Jay Thomson, Former President;

Suzanne Morin, Member of the Spam Committee.

Mr. Thomson made a presentation and, with Ms. Morin, answered questions.

At 12:23 p.m., it was agreed that the committee adjourn to the call of the Chair.

ATTEST:

PROCÈS-VERBAL

OTTAWA, le jeudi 6 mai 2004
(16)

[*Traduction*]

Le Comité sénatorial permanent des transports et des communications se réunit aujourd'hui, à 10 h 55, dans la salle 705 de l'édifice Victoria, sous la présidence de l'honorable Joan Fraser (*présidente*).

Membres du comité présents: Les honorables sénateurs Corbin, Day, Fraser, Graham, c.p., LaPierre, Merchant et Phalen (7).

Également présent: Terrance Thomas, attaché de recherche, Direction de la recherche parlementaire, Bibliothèque du Parlement.

Aussi présents: Les sténographes officiels du Sénat.

Conformément à l'ordre de renvoi adopté par le Sénat le mardi 23 mars 2004, le comité poursuit son examen du projet de loi S-2, Loi visant à empêcher la diffusion sur l'Internet de messages non sollicités.

TÉMOINS:

De l'Association canadienne des fournisseurs Internet:

Jay Thomson, ancien président;

Suzanne Morin, membre du comité sur le pourriel.

M. Thomson fait un exposé puis, aidé de Mme Morin, répond aux questions.

À 12 h 23, le comité suspend ses travaux jusqu'à nouvelle convocation de la présidence.

ATTESTÉ:

Le greffier du comité,

Till Heyde

Clerk of the Committee

EVIDENCE

OTTAWA, Thursday, May 6, 2004

The Standing Senate Committee on Transport and Communications met this day at 10:55 a.m. to examine Bill S-2, an Act to prevent unsolicited messages on the Internet.

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

[*Translation*]

The Chairman: I see we have a quorum. Welcome to all of you. We are resuming consideration of Bill S-2, the anti-spam bill.

[*English*]

Today we are fortunate to welcome representatives of the Canadian Association of Internet Providers, CAIP. They are Mr. Jay Thomson, former president of the association; and Suzanne Morin, who is a member of the association's spam committee.

I think you understand our normal procedure. We ask you to make an opening statement of maybe 15 minutes and then we go to a question period. If that is agreeable, I will give you the floor.

Mr. Jay Thomson, Former President, Canadian Association of Internet Providers: With me today is a member of CAIP's spam committee, Suzanne Morin. She is Assistant General Counsel, Regulatory Law, with Bell Canada. Ms. Morin has been very active in the policy area regarding spam. She has organized expert-level spam workshops through the Internet Law and Policy Forum, ILPF, as well as through the Global Business Dialogue On Electronic Commerce, GBDe. She was the key drafter for BCE of the GBDe's 2003 multilateral framework for addressing spam. As for me, although I am currently employed as Assistant Vice President, Broadband Policy, with TELUS Communications Inc., I was until February this year, president of CAIP.

CAIP represents all sectors of the Canadian Internet service provider industry. Our membership is made up of a broad and diverse group of Canadian Internet service providers, ISPs, including large, medium and small independent access providers, those who connect you to the Internet; incumbent and competitive telephone companies; backbone providers; wireless providers; and those companies who host Web sites, Web hosters. We appreciate the invitation to appear today to discuss spam and what Canada should be doing to address the problem. I read with great interest the transcript of Senator Oliver's appearance before the committee last week. I must commend him on the breadth and detail of his testimony, and members of this committee for their knowledge of the issue, which

TÉMOIGNAGES

OTTAWA, le jeudi 6 mai 2004

Le Comité sénatorial permanent des transports et des communications se réunit aujourd'hui à 10 h 55 pour étudier le projet de loi S-2, Loi visant à empêcher la diffusion sur l'Internet de messages non sollicités

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

[*Français*]

La présidente: Je vois qu'on a le quorum. Je vous souhaite à tous la bienvenue au comité. Nous poursuivons notre étude du projet de loi S-2, la Loi anti-pourriel.

[*Traduction*]

Nous avons la bonne fortune aujourd'hui de recevoir les représentants de l'Association canadienne des fournisseurs Internet, l'ACFI. Il s'agit en l'occurrence de M. Jay Thomson, ancien président de l'Association et de Mme Suzanne Morin qui est membre du comité sur le pourriel.

Vous connaissez je crois notre façon de procéder. Nous vous demandons de faire une déclaration préliminaire d'une quinzaine de minutes, après quoi nous aurons une période de questions. Si vous êtes d'accord, je vous laisse maintenant la parole.

M. Jay Thomson, ancien président, Association canadienne des fournisseurs Internet: Je suis accompagné aujourd'hui par une des membres de comité sur le pourriel, Mme Suzanne Morin. Mme Morin est conseillère générale adjointe en droit réglementaire chez Bell Canada, et elle a été très active dans le domaine de la politique concernant les pourriels. Elle a organisé des colloques spécialisés sur le sujet dans le cadre du Forum sur la politique et le droit relatifs à Internet ainsi que dans le cadre du dialogue mondial des entreprises sur le commerce électronique, que nous appelons le GBD. C'est elle qui a piloté, pour la BCE, l'élaboration de l'édition 2003 du Cadre de référence multilatéral de la GBD pour lutter contre les pourriels. En ce qui me concerne, même si je suis actuellement vice-président adjoint chargé de la politique de la bande large chez TELUS Communications Inc., j'étais jusqu'au mois de février le président de l'ACFI.

Notre association représente tous les secteurs de l'industrie canadienne des fournisseurs de services Internet. Nos membres représentent une palette très large et très variée de fournisseurs canadiens de service Internet, ce qu'on appelle les FSI, et notamment de petits, moyens et gros fournisseurs indépendants d'accès, ce qui vous permet de vous brancher sur Internet, les compagnies de téléphone titulaires et privées, des fournisseurs d'infrastructures, des fournisseurs de services sans fil ainsi que des fournisseurs de service d'hébergement Web. Nous sommes reconnaissants d'avoir été invités à venir vous parler aujourd'hui des pourriels et de ce que le Canada devrait faire pour contrer ce problème. J'ai lu avec beaucoup d'intérêt la transcription de la déposition du sénateur Oliver devant le comité

was clearly demonstrated in the questions posed to their colleague.

Senator Oliver has obviously done his homework. Based on his extensive research, he was able to offer you a host of statistics from numerous sources regarding the extent of the problem posed by spam and the impact it is having on Internet users in Canada and the world and on ISPs. Frankly, there is very little I can add to these data.

We all now know that spam is a problem, and a growing one. The question to be answered then is what do we do about it? To this end, it is important for the committee members to fully understand and appreciate that there is only one villain when it comes to spam, and that is the spammer. Everyone else in the Internet communications chain, in particular ISPs and end-users, are victims. Managing spam is extremely expensive for ISPs. Beyond the network bandwidth and storage costs it triggers, significant resources are applied to software and best-practice-development matters and customer-care activities. Many smaller CAIP members are seeing profits diminish to near zero as they attempt to deal with spam. ISPs have a vested interest in reducing spam and continue to invest in ways to address the problem. For this reason, we thank Senator Oliver for his efforts to increase public and political awareness of spam issues, and of the battle against spam the ISP industry has been fighting for years now. This battle requires engagement by many, and the attention of key policy-makers is critical. This committee has been asked to study Bill S-2, and presumably to come to some understanding of whether the proposed legislation would be an effective mechanism to achieve the laudable goal of reducing spam.

With all due respect, it is CAIP's position that a new, targeted anti-spam law is not the answer and could, we fear, detract from existing technological, commercial and legal mechanisms that are or could be put to use in the battle against spam.

We at CAIP favour a multi-faceted approach to addressing spam, which includes technology, industry self-regulation, consumer education, international cooperation and, on the legal front, the enforcement of existing domestic legislation. On this last point, several Internet experts, including Mr. Michael Geist of the University of Ottawa, whom you spoke of last week, have noted that the elements of most anti-spam legislation found in other jurisdictions can already be found in existing Canadian laws.

la semaine dernière, et je dois féliciter ce dernier pour la profondeur et le détail de son témoignage, tout comme je veux féliciter les membres du comité pour leur connaissance du sujet, comme en attestaient clairement les questions qu'ils ont posées à leur collègue.

Le sénateur Oliver a manifestement bien étudié la question. Fort de ses nombreuses recherches, il a pu vous fournir une foule de statistiques venant de sources multiples qui concernaient l'envergure du problème que représentent les pourriels et l'impact de ce problème sur tous ceux qui utilisent Internet au Canada et à l'étranger, ainsi que sur les FSI. Pour être franc avec vous, je n'ai pas grand-chose à ajouter à ces données.

Nous savons tous que les pourriels posent problème, un problème de plus en plus aigu. La question à poser est donc de savoir que faire pour contrer ce problème? Pour cela, il est impératif que les membres du comité comprennent parfaitement que lorsqu'on parle des pourriels, il n'y a qu'un seul coupable, et ce coupable c'est celui qui les produit. Tous les autres éléments de la chaîne Internet, en particulier les FSI et les utilisateurs, en sont les victimes. Il est extrêmement coûteux pour les FSI d'intervenir contre les pourriels. Outre les questions de largeur de bande du réseau et les frais de stockage qu'entraînent les pourriels, les FSI doivent consacrer énormément de ressources à l'amélioration des logiciels, à la mise au point de méthodes de pointe et aux activités de services à la clientèle. Un grand nombre de membres de l'Association qui travaillent à une échelle plus réduite voient leurs bénéfices pratiquement disparaître en raison des interventions qu'ils doivent mener pour contrer le problème des pourriels. Les FSI ont tout intérêt à faire disparaître les pourriels et ils investissent continuellement pour trouver des solutions au problème. Pour cette raison, nous remercions le sénateur Oliver de ses efforts pour sensibiliser davantage la population et les milieux politiques aux problèmes des pourriels et au combat que l'industrie mène depuis plusieurs années déjà sur ce front. Ce combat exige la mobilisation des nombreuses parties prenantes, et il est essentiel que les pouvoirs publics accordent leur attention au problème. Le comité a été saisi du projet de loi S-2 et on s'attend vraisemblablement à ce qu'il en arrive à déterminer si le projet de loi pourrait effectivement constituer un mécanisme utile pour contrer le phénomène des pourriels, objectif louable s'il en est.

En toute déférence, notre association estime qu'une nouvelle loi qui ciblerait expressément les pourriels n'est pas la solution et risque, nous le craignons fort, de nuire aux mécanismes technologiques, commerciaux et légaux qui existent déjà et qui sont ou pourraient être utilisés pour combattre le phénomène.

L'Association canadienne des fournisseurs Internet préconise plutôt de combattre les pourriels sur plusieurs fronts à la fois, notamment par la technologie, par l'autoréglementation de l'industrie, par l'éducation du consommateur, par la coopération internationale et, sur le plan juridique, par une rigoureuse application des lois déjà en vigueur au Canada. À ce dernier égard, plusieurs experts de l'Internet dont M. Michael Geist, de l'Université d'Ottawa, avec lequel vous vous êtes entretenus la semaine passée, ont signalé qu'on trouve déjà dans la législation canadienne des éléments de la plupart des lois antipourriels qui existent dans d'autres pays.

Specifically, existing domestic laws dealing with privacy, criminal matters and competition are capable of getting at the worst aspects of spam, those aspects that go beyond annoyance and drains on productivity.

These laws are capable of addressing the improper acquisition and use of personal e-mail addresses, criminally fraudulent conduct, dissemination of child pornography and deceptive marketing practices. Canada is not missing anti-spam laws. We are missing the targeted and aggressive enforcement of the laws we have.

Senators are aware that Industry Canada intends to soon issue a spam action plan. We understand that this action plan will also promote a multi-faceted approach to dealing with the spam problem, including the enforcement of existing laws. This is not idle talk. Both the public and private sectors are moving forward to formally explore how we can work together to enforce existing laws to fight spam.

A few years ago, the Government of Canada published its Cyberwise strategy for dealing with illegal and offensive content on the Internet. This strategy recognized that promoting the safe, wise and responsible use of the Internet is the responsibility of all interested and affected parties, including the Internet industries, other businesses, government and consumers. The same holds true for spam. Fighting it effectively will require multiple parties working together to deploy a combination of both existing and new strategies.

We are concerned that targeted anti-spam legislation represents a "silver bullet" approach that risks raising unrealistic consumer expectations. Spam is not something we can magically legislate away; and we have proof of this. As the committee knows, a number of jurisdictions have passed their own, new anti-spam laws and yet the volume of spam continues to increase. It is clear that simply making spam illegal will not make it disappear.

We are concerned that targeted anti-spam legislation in Canada could impede rather than assist in the battle against spam, should it serve to prejudge or direct efforts away from assessment of and experimentation with broadly based anti-spam tactics. Perhaps more importantly, today's perceived solutions will likely be ineffective in addressing tomorrow's problems. We all know how fast technology is changing. The nature of spam and the tactics spammers employ are changing just as quickly. By the time specific, targeted anti-spam legislation was passed, it would likely be outdated. This is another reason why we favour the application and enforcement of more generally applicable

Pour être plus précis, les lois canadiennes qui concernent la protection de la vie privée, la lutte contre les activités criminelles et la concurrence pourraient fort bien éradiquer les aspects les plus nuisibles du phénomène, les aspects qui transcendent le simple inconvénient et nuisent à la productivité.

Ces lois pourraient permettre de contrer l'acquisition et l'utilisation abusives d'adresses courriels privées, les actes criminels frauduleux, la diffusion de pornographie infantile et les pratiques commerciales frauduleuses. Le Canada ne manque pas de lois antipourriels. Ce qui nous manque, c'est une application rigoureuse et bien ciblée des lois que nous avons déjà.

Les sénateurs savent qu'Industrie Canada entend déposer bientôt un plan d'action antipourriels. Nous croyons savoir que ce plan d'action va également préconiser des interventions sur plusieurs fronts pour contrer le phénomène des pourriels, et notamment une application plus rigoureuse des lois existantes. Ce ne sont pas là de vains mots. Le secteur public comme le secteur privé vont résolument de l'avant afin de déterminer de façon formelle comment il leur serait possible de travailler en coopération pour combattre le phénomène des pourriels par une application plus rigoureuse des lois existantes.

Il y a quelques années, le gouvernement canadien a publié sa stratégie Cyberberaverti pour faciliter la lutte contre la diffusion de matériels illégaux ou de mauvais goût sur Internet. Cette stratégie reconnaissait qu'il appartient à toutes les parties intéressées et affectées, c'est-à-dire notamment l'industrie de l'Internet, l'entreprise en général, les pouvoirs publics et les consommateurs, d'encourager une utilisation sécuritaire, avertie et responsable d'Internet. Il en va de même pour les pourriels. Pour combattre efficacement ce phénomène, il faudrait que toutes les parties travaillent de concert pour mettre en oeuvre une palette de stratégies existantes et nouvelles.

Nous craignons qu'une loi antipourriels spécifique ne soit présentée comme un genre de potion magique risquant de produire des attentes irréalistes chez le consommateur. Le pourriel n'est pas quelque chose qu'on peut faire disparaître comme par magie grâce à une loi, et nous en avons la preuve. Comme le comité le sait déjà, plusieurs pouvoirs publics ont déjà adopté des lois antipourriels, ce qui n'a pas empêché le volume des pourriels de continuer à augmenter. Il est évident que ce n'est pas en mettant les pourriels hors la loi qu'on les fera disparaître.

Nous craignons que l'adoption par le Canada d'une loi antipourriels spécifique n'entrave la lutte contre le pourriel au lieu de la faciliter si elle sert à éloigner ou à détourner les efforts déployés pour évaluer et mettre à l'essai des tactiques antipourriels tous azimuts. Ce qui peut être plus important encore, ce qui passe aujourd'hui pour des solutions risque d'être inefficace face aux problèmes de demain. Nous savons tous à quel point la technologie évolue rapidement. La nature même des pourriels et les tactiques utilisées par ceux qui les produisent évoluent tout aussi rapidement. D'ici qu'une loi antipourriels spécifique soit adoptée, elle sera probablement dépassée. Voilà

laws as one of the items on the anti-spam menu that Canada should adopt.

In respect of other items on this menu, there are myriad technical and commercial anti-spam activities currently underway. For example, network- or server-based filtering technology and techniques continue to improve. At the same time, consumer awareness and understanding of user-controlled filters are also improving. These efforts are resulting in extremely large proportions of spam being blocked before they ever hit a user's inbox. Numerous industry and international working groups exist to share strategies and information — for example, who the spammers are — and work toward common standards. Many CAIP members are active in these groups.

Industry and international activities, such as the "secure your server" initiative, are geared toward service providers and others whose systems might be susceptible to remote hijacking for purposes of sending spam. Similarly, increased user education and adoption of firewalls and anti-virus programs are geared toward protecting end-user computers from being hijacked for similar purposes. Almost all ISPs actively promote firewall and anti-virus services; some even include the services at no charge to their high-speed Internet customers.

Many ISPs, for economic reasons and to ensure continued receipt of their transmissions by other ISPs in the communication chain, actively explore opportunities to block spam before it leaves their network. That is to say, they are blocking the spammer at the source.

In closing, allow me to assure the committee that ISPs, on behalf of their customers and out of clear self-interest, are and will remain the most aggressive of spam fighters. Our contribution to the battle need not be compelled by targeted legislation, regulation or licensing. Canada's laws of general application, most notably those dealing with privacy and criminal and deceptive practices, are capable, with enhanced enforcement, of addressing the worst aspects of spam. Canada's domestic anti-spam efforts should be focused on enforcing existing laws and not on making new laws. The fruits of Senator Oliver's efforts will no doubt be at the heart of Industry Canada's anticipated anti-spam program. We urge you to wait for that process to unfold before pursuing new legislation in this area.

également pourquoi nous préconisons plutôt une application rigoureuse de lois de portée plus générale qui seraient l'un des nombreux éléments au menu de la lutte contre les pourriels dont le Canada devrait se doter.

S'agissant des autres éléments de ce menu, il y a une myriade d'activités techniques et commerciales destinées à contrer les pourriels qui sont actuellement en cours d'exécution. Ainsi, les techniques de filtrage implantées au niveau des réseaux ou des serveurs n'arrêtent pas de s'améliorer. Simultanément, le consommateur est de plus en plus au courant de l'existence de ces filtres dont il a le contrôle et il comprend mieux comment les utiliser. Tous ces efforts font qu'un pourcentage considérable des pourriels peuvent être bloqués avant même d'arriver dans la boîte aux lettres de l'utilisateur. Il existe également dans l'industrie et au niveau international un grand nombre de groupes de travail qui s'échangent de la stratégie et de l'information, — notamment en ce qui concerne l'identité des producteurs de pourriels, qui travaillent ensemble pour élaborer des normes communes. Bon nombre des membres de l'Association sont actifs au sein de ces groupes de travail.

Et les activités pilotées par l'industrie et menées au niveau international, par exemple l'initiative «sécurisez votre serveur», sont axées sur les fournisseurs de services et tous ceux dont le système pourrait être vulnérable aux pirates qui voudraient s'en servir pour diffuser des pourriels. Parallèlement, une meilleure sensibilisation des utilisateurs ainsi que l'adoption de coupe-feu et de programmes antivirus ont pour but de mieux protéger les ordinateurs des utilisateurs contre ce genre d'activités de piratage. Pratiquement tous les FSI encouragent activement les utilisateurs à installer des coupe-feu et des logiciels antivirus; certains offrent même gratuitement ce service à ceux de leurs clients qui s'abonnent à un service Internet à grand débit.

Pour des raisons économiques mais également pour pouvoir continuer à recevoir les transmissions des autres FSI, qui font partie de la chaîne de nos communications, ces derniers sont nombreux à explorer tous les moyens possibles de bloquer les pourriels avant que ceux-ci ne quittent leur réseau. Cela veut dire qu'ils bloquent ainsi ces pourriels à la source.

Pour terminer, permettez-moi de donner au comité l'assurance que les FSI, agissant pour le compte de leurs clients mais également dans leur intérêt manifeste, sont et demeureront les plus ardents ennemis des pourriels. Le rôle que nous jouons dans la bataille ne doit pas être un rôle forcé, imposé par une loi, des règlements ou un processus d'octroi de licences spécifiques. Les lois canadiennes d'application générale, et en particulier en ce qui concerne la protection de la vie privée, la lutte contre le crime et les pratiques frauduleuses, peuvent déjà, pourvu qu'elles soient plus rigoureusement appliquées, déjouer les aspects les plus nuisibles du phénomène des pourriels. Les initiatives prises au Canada pour lutter contre les pourriels devraient être axées plutôt sur une application rigoureuse des lois existantes que sur l'élaboration de nouvelles lois. Le fruit des efforts du sénateur Oliver se retrouvera indubitablement au coeur du programme antipourriels que nous attendons de la part d'Industrie Canada. Nous vous exhortons à attendre l'aboutissement de ce processus avant d'envisager de légiférer dans ce domaine.

We would be pleased to respond to your questions.

Senator Corbin: Mr. Thomson, do you remain in contact on an ongoing basis with Industry Canada parties interested in this issue?

Mr. Thomson: Yes, we certainly do that. We have been active at CAIP in consultations with Industry Canada. Industry Canada issued a discussion paper a little over one year ago. We were active participants in responding to that paper. We have been in contact with their officials since the process was undertaken. We have talked to them about their spam action plan. We look forward to continuing to work with them when that action plan is rolled out.

Senator Corbin: Is there a document available on the outcome of those discussions between Industry Canada and your industry?

Mr. Thomson: There is no —

Senator Corbin: In other words, has there been progress in terms of the industry's and government's efforts to deal with this issue?

Mr. Thomson: I think it is safe to say that the spam action plan will be the result of the discussions that have taken place to date. It will outline the various positions presented and will propose a plan to deal with spam based on the consultations that government had with numerous parties, including CAIP.

Senator Corbin: I have the impression from you, and from Senator Oliver's comments last week on the apparent reticence of Industry Canada, that there is a considered effort to kill Senator Oliver's attempt to deal with this. Is that a correct assessment? You used quite strong words this morning in that respect. You quoted Dr. Michael Geist, for example, who said that existing domestic legislation covers the waterfront and so we do not need anything else.

Mr. Thomson: I think it is safe to say, as I indicated in my remarks, that we do not support new legislation in this area and that we feel quite strongly that the existing laws should be enforced aggressively. We could then assess how well that works before we introduce new legislation, whether it is Senator Oliver's bill or any other bill.

Senator Corbin: However, the Internet users among the consumer public are becoming rather impatient with the perceived inability of industry to put a stop to spam. You invoked complicated technical matters, agreements with providers in other arenas and so on, but how much longer will the user, who pays for this service and expects a clean signal, have to wait before there is a resolution of the problem? Is that not what Senator Oliver is attempting to do with this bill — push things forward?

Nous répondrons avec plaisir à vos questions.

Le sénateur Corbin: Monsieur Thomson, êtes-vous en contact permanent direct avec les services d'Industrie Canada qui s'occupent de ce dossier?

M. Thomson: Absolument. Au niveau de l'Association, nous nous sommes employés à consulter activement Industrie Canada. Le ministère a produit il y a un peu plus d'un an un document de discussion, auquel nous nous sommes empressés de répondre. Nous sommes en rapport avec les fonctionnaires d'Industrie Canada depuis le tout début du processus. Nous leur avons parlé du plan d'action antipourriels d'Industrie Canada et nous nous réjouissons de pouvoir continuer à travailler avec eux lorsque ce plan d'action sera dévoilé.

Le sénateur Corbin: Existe-t-il un document quelconque sur l'issue de ces discussions entre Industrie Canada et vous?

M. Thomson: Il n'y a pas...

Le sénateur Corbin: En d'autres termes, les efforts déployés par l'industrie et par le gouvernement dans ce dossier ont-ils permis de faire des progrès?

M. Thomson: Je pense qu'on peut dire sans risque de se tromper que le plan d'action antipourriels sera la résultante des discussions qui ont eu lieu jusqu'à présent. Ce plan exposera les diverses positions qui ont été exprimées et proposera une stratégie antipourriels qui reposera sur les consultations qui ont eu lieu entre le gouvernement et de nombreux intervenants comme l'ACFI.

Le sénateur Corbin: J'ai l'impression, à vous entendre et à entendre le sénateur Oliver qui parlait la semaine dernière de la réticence que semble avoir Industrie Canada, qu'on s'efforce délibérément de tuer dans l'oeuf ce que le sénateur Oliver essaie de faire pour remédier au problème. Cette impression est-elle fondée? En parlant de cela ce matin, vous n'avez pas mâché vos mots. Vous avez notamment cité le professeur Michael Geist qui nous a dit qu'au Canada, la législation existante couvrait bien le terrain et que donc nous ne devions pas faire quoi que ce soit d'autre.

M. Thomson: Je dirais qu'effectivement, comme je l'ai signalé dans ma déclaration, on peut affirmer que nous ne sommes pas favorables à une nouvelle loi dans ce domaine et que nous avons l'intime conviction qu'il faudrait plutôt faire appliquer rigoureusement les lois existantes. En faisant cela, on pourrait alors déterminer si ces lois sont vraiment opérantes avant d'envisager d'en présenter une nouvelle, qu'il s'agisse du projet de loi du sénateur Oliver ou de toute autre mesure législative.

Le sénateur Corbin: Cependant, les utilisateurs d'Internet qui font partie des consommateurs commencent à s'impatienter parce qu'ils ont l'impression que l'industrie est incapable d'arrêter le phénomène des pourriels. Vous avez parlé de questions techniques complexes, d'accords avec les fournisseurs dans d'autres secteurs et ainsi de suite, mais combien de temps encore l'utilisateur, qui après tout paie pour avoir ce service et qui compte sur un signal propre, devra-t-il attendre avant que ce problème soit réglé une fois pour toutes? N'est-ce pas précisément cela que le sénateur Oliver essaie de faire avec son projet de loi, faire bouger les choses?

Ms. Suzanne Morin, Member of the Spam Committee, Canadian Association of Internet Providers: I absolutely agree that Senator Oliver's bill has pushed things forward and helped encourage Industry Canada to move forward with their action plan.

We have also been waiting for Industry Canada's action plan. It has taken a little time to come out, maybe longer than we would have liked. I do not think it is a secret that industry players have been encouraging Industry Canada to issue their action plan, which we hope will come out soon. The multi-faceted approach that we think will be in that action plan is something that we have been advocating for a couple of years now, both domestically and internationally.

A few years ago, some ISPs thought we needed new legislation to beat this problem. It is killing us — it is affecting our business and our customers. We went through an exercise to look at the different pieces of legislation that countries have introduced and saw that the kinds of things they were making illegal were actually covered in our legislation as well. I think Canada was also under some pressure in the last year to be seen to be doing something on the legislative front.

Obviously things do not happen that quickly, which is why we have taken a very strong position that we would like to begin, and continue to push, the dialogue on this issue, speak with various law enforcement agencies that have a role to play, and cooperate with them to the extent that ISPs can. At the same time, we want to continue our other efforts on the technology side, including cooperating with other ISPs to keep spam from leaving our networks, but also from entering our networks. Because it is such an international problem, it has taken an international pace to get some of these things in place.

Senator Corbin: I know that we will hear from Industry Canada eventually, but are you suggesting that they could speed things up? Are they dragging their feet? Let us be open about it.

Ms. Morin: It would be nice to have it out today, yes.

The Chairman: Are you suggesting that for some reason, they have been dragging their feet, to use Senator Corbin's phrase, or is this the normal slow working of bureaucracy?

Ms. Morin: I would put it more in the latter category, because our discussions with them have been ongoing. I would not want to cast any aspersions on what Industry Canada may or may not be doing. However, we would definitely like to have it out sooner rather than later.

Mme Suzanne Morin, membre du comité sur le pourriel, Association canadienne des fournisseurs Internet: Je suis tout à fait d'accord pour dire que le projet de loi du sénateur Oliver a fait bouger les choses et a permis d'encourager Industrie Canada à aller de l'avant avec son plan d'action.

Nous aussi, nous attendons le plan d'action d'Industrie Canada. Il a fallu un peu de temps avant de le voir, peut-être plus longtemps que nous ne l'aurions voulu, mais ce n'est je crois un secret pour personne que l'industrie a vivement encouragé Industrie Canada à déposer son plan d'action, et nous espérons que ce sera bientôt fait. L'intervention sur plusieurs fronts que préconisera croyons-nous ce plan d'action est précisément quelque chose que nous recommandons déjà depuis un ou deux ans, à la fois au Canada et à l'étranger.

Il y a quelques années, certains fournisseurs pensaient qu'il fallait une nouvelle loi pour combattre le phénomène, un problème qui nous tue littéralement et qui affecte à la fois notre chiffre d'affaires et nos clients. Nous nous sommes employés à examiner les lois qui existent dans les autres pays et nous avons constaté que tout ce qu'ils avaient rendu illégal l'était également au Canada. Je pense que depuis un an, le Canada fait également l'objet de certaines pressions pour qu'il donne l'impression de faire quelque chose sur le plan législatif.

Mais de toute évidence, les choses ne se passent pas aussi rapidement que cela, et c'est la raison pour laquelle nous avons fermement pris position en disant que nous aimerions entamer, en continuant à insister à ce sujet, le dialogue dans ce dossier, en parlant aux différents corps policiers qui ont un rôle à jouer et en coopérant avec eux dans toute la mesure de nos moyens. Simultanément, nous voulons poursuivre ce que nous faisons déjà par ailleurs sur le plan de la technologie, notamment en coopérant avec les autres fournisseurs de manière à empêcher les pourriels de sortir de nos réseaux, mais également d'y entrer. Étant donné la dimension internationale du problème, il a fallu des pressions internationales pour arriver à mettre certains de ces éléments en place.

Le sénateur Corbin: Je sais que nous allons à un moment donné entendre les représentants d'Industrie Canada, mais ne voulez-vous pas nous dire ici que le ministère pourrait un peu accélérer le rythme? Se traîne-t-il les pieds? Disons les choses franchement.

Mme Morin: Ce serait bien si le plan d'action était déposé aujourd'hui, c'est certain.

La présidente: Voulez-vous dire que pour une raison ou une autre, le ministère s'est traîné les pieds, pour reprendre l'expression du sénateur Corbin, ou s'agit-il d'une lenteur normale dans la bureaucratie?

Mme Morin: Ce serait probablement une lenteur normale étant donné que nous n'avons jamais arrêté nos discussions avec le ministère. Je ne voudrais pas jeter le discrédit sur ce que fait ou ne fait pas Industrie Canada, mais il est certain que nous préférerions que le plan d'action soit rendu public aussi rapidement que possible.

Mr. Thomson: It may be a matter of bureaucracy in the face of a pending election call.

Senator Corbin: I have one last comment. What is it about Senator Oliver's bill specifically that you resent?

Mr. Thomson: The starting point is that we think any new legislation is unnecessary at this time. With respect to Senator Oliver's bill, we have a number of concerns about how it is drafted. For example, the preamble outlines the premise on which the bill is based — that is, that the regulation and licensing of Internet service providers will actually help to solve the problem of spam. We think that is the wrong approach and the wrong beginning.

There are concerns about the concept of a no-spam list. We do not think it would be effective. It would impact on legitimate e-mail marketers, but the hard-core spammers will ignore it, as they have other laws in other jurisdictions. There is a concern that the list may ultimately become available to spammers through security leaks, thus giving them a great list to use.

Senator Corbin: What is the line between legitimate and illegitimate e-mail sources?

Ms. Morin: It depends on the context. Some of the spammers think their spam is legitimate. If you look at the different characteristics, what people usually think of when they refer to spam is what we would call the nasty and annoying stuff — the fraudulent matter, the get-rich-quick schemes, the pornography, body part enlargements, all of those types of things.

Senator Corbin: You are getting into the field of morality.

Ms. Morin: It is things people have not asked for but are receiving. There is another layer of legitimate marketing, in the sense that what they are trying to sell you are legitimate products and services, but how did they obtain your e-mail address? That gets more into privacy considerations.

You did speak last week about opt-in versus opt-out approaches — and why the U.S. chose the approach of opting out versus the European approach of opting in. In Canada, we have an opt-in approach when it comes to sending unsolicited commercial e-mail. If there is no pre-existing customer relationship, then the expectation is that the marketing association will wait until they have consent from the individual — until that individual opts in to receiving e-mail from them. Therefore, in essence, we have an opt-in approach.

M. Thomson: Peut-être s'agit-il également d'une réaction normale de la bureaucratie à la veille du déclenchement imminent des élections.

Le sénateur Corbin: Je voudrais dire une dernière chose. Qu'est-ce que vous n'aimez pas dans le projet de loi du sénateur Oliver?

M. Thomson: Pour commencer, nous estimons qu'une nouvelle loi est inutile pour l'instant. En ce qui concerne maintenant le projet de loi du sénateur Oliver, nous avons quelques réserves concernant son texte. Ainsi, le préambule évoque le postulat sur lequel repose le projet de loi, en l'occurrence le fait que réglementer les fournisseurs de service Internet et leur imposer des licences permettrait en partie de régler le problème des pourriels. Nous pensons que ce n'est pas la bonne façon de procéder et que ce n'est pas ainsi qu'il faut commencer.

Nous avons également quelques réserves au sujet de l'idée d'une liste de ce qui ne constitue pas des pourriels. Nous ne pensons pas que cela puisse marcher. Une telle disposition aurait un impact sur les exploitants licites, mais les polluposteurs invétérés n'en auront cure, tout comme ils font fi des lois qui existent ailleurs. Il est à craindre que cette liste finisse par tomber entre les mains des polluposteurs suite à l'une ou l'autre faiblesse des systèmes de sécurité, ce qui leur donnerait une liste extrêmement utile.

Le sénateur Corbin: Quelle est la distinction entre une source licite et une source illicite de courriel?

Mme Morin: Tout dépend du contexte. Certains polluposteurs pensent que leurs pourriels sont parfaitement légitimes. Si vous regardez les caractéristiques de la chose, en règle générale, lorsqu'un consommateur parle de pourriel, il pense généralement à des choses que nous qualifierons de déplaisantes ou de gênantes, tout ce qui est frauduleux, les combines pour devenir riche, la pornographie, les produits pour développer certaines parties du corps, ce genre de choses.

Le sénateur Corbin: Mais on entre ici dans le domaine de la moralité.

Mme Morin: Ce sont toutes les choses que le consommateur n'a pas sollicitées mais qu'il reçoit néanmoins. Il y a une autre catégorie de publicité légitime, celle qui vise des produits et des services légitimes que les expéditeurs essaient de vous vendre, mais il faut alors se demander comment ils ont réussi à obtenir votre adresse électronique. Et cela relève davantage de la protection de la vie privée.

La semaine dernière, vous avez évoqué les deux options, l'option d'acceptation et l'option de refus, et vous avez dit pourquoi les États-Unis avaient choisi l'option de refus alors que les Européens ont préféré l'autre. Au Canada, nous avons opté pour la formule de l'acceptation en ce qui concerne l'envoi de courriel non sollicité à caractère commercial. S'il n'existait auparavant aucun rapport quel qu'il soit entre l'expéditeur et le client potentiel, on s'attend alors à ce que l'organisme qui fait le marketing attende d'avoir obtenu le consentement de la personne en question, c'est-à-dire qu'il ait expressément choisi d'accepter ses courriels. Par conséquent, nous avons essentiellement ici l'option de l'acceptation expresse.

Furthermore, many marketers in Canada will only send electronically — telemarketing is different because e-mail has a different sensitivity to it — commercial e-mail to you if you have opted into their distribution list. There again, the medium has required more active participation on the part of the person receiving the e-mail.

In the U.S., they have an opt-out approach. There is a small component of that in Senator Oliver's bill as well, in that the approach they have taken in the U.S. is to tell you what you need to do in order to make your spam legitimate. It may still be unwanted. It actually allows every company in the U.S. to send you one e-mail until you tell them to stop. I do not know the numbers; but if every company in the U.S. sent every individual in the U.S. an e-mail in accordance with the CAN-SPAM Act — which says, "I will not hide who I am, I will allow you to opt out," has the appropriate headers, all of those things — you would get hundreds of e-mails a day anyway, and each individual would have to tell each one of those companies to stop. That is not what we think the approach should be.

That is an exaggeration, because not every company in the U.S. would do that. However, if taken to the extreme, that is what would happen. There is a little of that in Senator Oliver's bill as well.

One of the bill's other aspects is the notion of putting in a header that this is an advertisement. If I am sending an e-mail on behalf of a company to my customers, I would like to have flexibility in how I will market. Some days, I might use something in the header to let them to know what this is about — it might be a contest or something else — but this, again, is for unsolicited commercial e-mail. Putting in "ADV" as short for advertisement, for example, will not stop the spammers, but it will force legitimate commercial e-mailers to add additional words in their marketing campaigns to their customers. Again, it adds an onus on legitimate marketers and does not actually help stop the spam.

Senator Corbin: Thank you very much.

Senator Graham: I have a supplementary housekeeping-type question to put things in focus so we have an idea of what organizations you represent. I know that, in broad terms, CAIP represents TELUS and Bell. Could you give me an idea of the number of companies, and then send us a list of them, so we have it for our records? We represent five different provinces as senators around the table, and I am sure we would all be interested to know if we have any members in our own backyards, apart from the national perspective that we get from both TELUS and Bell.

Par ailleurs, il y a au Canada beaucoup d'entreprises qui n'envoient aux consommateurs des courriels — et ce n'est pas la même chose pour le télémarketing parce que la formule du courriel n'a pas du tout la même réactivité — des courriels à caractère commercial si vous avez expressément accepté d'être sur leur liste de distribution. Là encore, ce mode de vente exige une participation plus active de la part du destinataire du courriel.

Les États-Unis ont pour leur part opté pour la formule du refus. On en trouve également un petit élément dans le projet de loi du sénateur Oliver, en ce sens que la formule adoptée aux États-Unis consiste à dire à l'expéditeur ce qu'il doit faire pour que son pourriel soit légitime. Mais même légitime, ce pourriel risque toujours d'être indésirable. Mais ce régime permet à toutes les entreprises américaines de vous envoyer un courriel jusqu'à ce que vous leur ordonniez d'arrêter. Je ne connais pas les chiffres, mais si chaque entreprise américaine envoyait à chaque Américain un courriel conforme aux dispositions de la CAN-SPAM Act — qui dit: «Je ne cache pas qui je suis, mais je vous permets de refuser» avec toutes les mentions appropriées et ce genre de choses — chaque Américain recevrait chaque jour des centaines de courriel et chaque Américain devrait ordonner à chacune de ces entreprises d'arrêter. Ce n'est pas ainsi qu'il faut faire les choses à notre avis.

C'est bien sûr une exagération, parce que ce ne sont pas toutes les entreprises américaines qui procéderaient ainsi. Par contre, si on pousse les choses à l'extrême, c'est exactement ce qui se produirait. Et on ne trouve pas grand chose de cela dans le projet de loi du sénateur Oliver.

On trouve également dans ce projet de loi la notion voulant qu'il faille un avis disant qu'il s'agit d'une publicité. Si j'envoie un courriel à mes clients pour le compte d'une entreprise, j'aimerais avoir une certaine latitude quant à la façon de présenter mon produit. Il pourrait arriver que je veuille mettre en bannière quelque chose qui permette à mes clients de savoir de quoi il s'agit — un concours ou quoi que ce soit d'autre — mais ici encore, il s'agit de courriels non sollicités à caractère commercial. Le fait d'afficher «PUB» pour dire qu'il s'agit d'une publicité, cela n'arrêtera pas les polluposteurs, mais cela contraindra les expéditeurs commerciaux légitimes à dire d'autres choses dans les campagnes de publicité à l'intention de leurs clients. Ici encore, ce sera une obligation supplémentaire imposée aux entreprises légitimes, mais cela ne fera rien pour arrêter le phénomène des pourriels.

Le sénateur Corbin: Merci beaucoup.

Le sénateur Graham: J'aurais une question complémentaire d'intérêt courant à poser pour nous donner une meilleure idée des organismes que vous représentez. Je sais que d'une façon générale, l'ACFI représente TELUS et Bell. Mais pouvez-vous me donner une idée du nombre de compagnies qui font partie de l'Association et nous en envoyer la liste ultérieurement, afin que cela figure dans nos dossiers? Les sénateurs qui siègent ici aujourd'hui représentent cinq provinces différentes, et je sûr que nous aimerions tous savoir si certains de vos membres évoluent dans notre cour, en plus bien sûr des intervenants comme TELUS et Bell qui offrent une perspective nationale.

Mr. Thomson: CAIP has approximately 100 members, including Bell, TELUS, AOL Canada, Sprint, Allstream and MCI Canada as the largest members, and IBM, Yahoo Canada and some 90-odd smaller ISPs spread across the country. CAIP members provide approximately 80 per cent of the Internet connections in Canada.

The Chairman: Please send us a list of your members.

Senator Phalen: I would like to ask a supplementary to Senator Corbin's questions and make sure that I understand this. If there were what I would call legitimate spam from a community organization or church that included the words "sex," "drugs" or "pornography," is that filtered out?

Ms. Morin: Today, service providers use many different spam filters. ISPs use their own filters. They will create their own and try to weed out words such as those you cited.

Senator Phalen: I wonder where you can draw the line?

Ms. Morin: Actually, there is nowhere that you can draw the line. The whole intent is to try to allow mail that is supposed to get through to get through and stop unwanted mail from getting through. I cannot guarantee that we will be 100-per-cent successful. I can also tell you that sometimes, depending on the filtering technology and software being used, unfortunately, e-mail that is intended to get through also gets blocked, because humans created the software but the software is making the decisions. We call these false positives. It could be, for example, an e-mail about breast cancer. Depending on the filtering technology you use, if you filtered all the e-mails with the word "breast" included, it would filter that out. I think that the software is becoming much more intelligent. Spammers will introduce ways to try to fool the filters. They will write "breast" with "b" and an asterisk, et cetera, to try to make it look like it is not the word that is being filtered out. Unfortunately, the technology today cannot solve 100 per cent of the problem. Filters are being improved and other techniques are being developed.

Mr. Thomson: Certain spam filters can be combined with the white-list approach, which allows the end-users to identify the sources from which they are willing to accept messages. If users put their church on the white list, then those messages will come through, notwithstanding that they might include some words that would otherwise cause them to be filtered out.

Senator Phalen: As senators, we would like to get rid of spam in one sense, but the other side of the coin is that we have to listen to the message that are coming. Where do you draw the line? Can you draw the line? I guess that is my line of thinking.

M. Thomson: L'ACFI compte une centaine de membres dont Bell, TELUS, AOL Canada, Sprint, Allstream et MCI Canada qui en sont les membres les plus importants, mais aussi IBM, Yahoo Canada et environ 90 petits fournisseurs de service Internet qui sont implantés un peu partout au Canada. Les membres de l'association produisent environ 80 p. 100 de toutes les liaisons internet au Canada.

La présidente: Vous voudriez bien nous envoyer la liste de vos membres.

Le sénateur Phalen: Je voudrais poser une question qui fait suite aux questions du sénateur Corbin et essayer de comprendre vraiment de quoi il s'agit. Si un organisme communautaire ou une église envoie ce que j'appellerais un pourriel légitime contenant des mots comme «sexe», «drogues», ou «pornographie», ces messages seraient-ils bloqués?

Mme Morin: À l'heure actuelle, les fournisseurs de services utilisent différentes sortes de filtres antipourriels. Chacun a les siens propres. Ils les créent pour essayer d'éliminer les messages qui contiennent des termes comme ceux que vous avez mentionnés.

Le sénateur Phalen: Mais je me demande jusqu'où on peut aller?

Mme Morin: En fait, il est impossible de tracer une ligne de démarcation. Tout ce qu'on veut, c'est d'essayer de permettre l'acheminement des pourriels qui sont censés pouvoir passer et d'arrêter les courriels non sollicités. Je ne peux pas vous garantir que nous ne pourrons jamais y arriver à 100 p. 100. Je peux également vous dire que parfois, selon le genre de méthode et de logiciel de filtrage qui est utilisé, il arrive malheureusement qu'un courriel qui était censé pouvoir être acheminé est arrêté étant donné que ce sont des êtres humains qui créent les logiciels mais que ce sont les logiciels qui décident. Nous appelons cela des faux positifs. Un bon exemple serait un courriel concernant le cancer du sein. Une méthode de filtrage pourrait fort bien bloquer tous les courriels contenant le mot «sein». Je pense que les logiciels deviennent de plus en plus intelligents. Les polluposteurs trouveront toujours le moyen de vaincre les filtres. Par exemple, au lieu d'écrire «sein», ils vont écrire «sein» afin de déjouer le filtre. Malheureusement, la technologie actuelle est incapable de remédier à 100 p. 100 au problème. Mais les filtres sont sans cesse perfectionnés et il y a également d'autres méthodes qui apparaissent.

M. Thomson: Certains filtres antipourriels peuvent être combinés à une liste blanche qui permet aux utilisateurs de donner les sources dont ils acceptent les messages. Ainsi, si un utilisateur met son église sur la liste blanche, les messages de l'église vont passer même si ces messages comportent certains mots qui auraient sinon entraîné leur blocage.

Le sénateur Phalen: Il est certain que, étant sénateurs, nous aimerions bien pouvoir nous débarrasser des pourriels, mais le revers de la médaille est que nous devons quand même écouter les messages qui nous parviennent. Où donc tracer la ligne de démarcation? Et peut-on en tracer une? C'est ainsi que je raisonne, dirais-je.

We hear about the high cost of spam in terms of lost productivity and increasing the bandwidth. Who pays for blocking spam? Is it the Internet user? If so, what is the cost?

Mr. Thomson: Ultimately, as in any other business, costs incurred by an Internet service provider are passed on to its customers in one way or another. That being said, Canada is known for having some of the lowest prices for Internet services in the world, and it is a very competitive marketplace. There is a strong expectation amongst Canadians that they will get their Internet service for a certain price. For a dial-up connection it has to be $20 or less. That is what they have become used to, and that is what they expect. In many cases, because it is a competitive environment, the ISP will absorb the costs and not pass them on directly to its customers. The ISP will instead have a lower margin, but that way it keeps the customers and keeps the business in a competitive marketplace.

Senator Merchant: You said that the U.S. is using the opt-out approach. Is that because the U.S. is the ultimate capitalist society? Do you have a preference for one system or the other?

Ms. Morin: We do have a preference in Canada. We have privacy legislation — it was referred to last week — the Personal Information Protection and Electronic Documents Act. It requires consent for the use of an individual's personal information. An e-mail address falls into that category in most instances. The form of consent you use will depend on the sensitivity of the information and the context. It is fair to say that people would agree that the use of their e-mail address is fairly sensitive because of the problem of spam. Ten years ago, when e-mail first came out, it might not have been, because if I was only getting five e-mails, I might not mind getting just one more. Expectations are very different today, not only for the use of e-mail but also instant messaging or receiving messages on your cell phone. People want to give permission before they start to get those, hence the opt-in approach. Essentially, that is what those who are serious about complying with these requests use here in Canada. In the U.S., the opt-out approach has been their way for many years, not just as it relates to spam and e-mail, but to privacy generally. Their preference for the opt-out approach goes back to privacy principles generally, where they prefer to assume they have your consent until you tell them otherwise, and so they have extended that same approach to the e-mail context.

They also generate over 50 per cent of the spam in the world. There is money to be made there. Obviously these people are paying someone. There are more targets and also more people to

On nous dit que les pourriels coûtent très cher parce qu'ils nuisent à la productivité et qu'ils obligent à élargir la largeur de la bande. Mais qui paye pour le filtrage des pourriels? Est-ce l'utilisateur? Et dans l'affirmative, combien cela coûte-t-il?

M. Thomson: Au bout du compte, comme dans toute activité commerciale, les frais généraux d'un fournisseur d'Internet finissent par se répercuter d'une façon ou d'une autre sur le consommateur. Cela dit, il est bien connu que le Canada est l'un des pays où les services Internet coûtent le moins cher au monde, et il s'agit d'un marché très concurrentiel. Les Canadiens s'attendent vraiment à payer un certain prix pour un service Internet. Pour une connexion par composition, ils s'attendent à payer au maximum 20 $. C'est ce qu'ils ont pris l'habitude de payer, et c'est ce à quoi ils s'attendent. Bien souvent, comme il s'agit d'un marché très concurrentiel, le fournisseur absorbe le coût et ne le répercute pas directement sur le consommateur. Il acceptera une marge bénéficiaire plus basse, mais ainsi il conservera son client et il restera concurrentiel.

Le sénateur Merchant: Vous avez dit que les États-Unis utilisent la formule du refus. Cela est-il dû au fait que les États-Unis sont la société capitaliste par excellence? Lequel des deux systèmes préférez-vous?

Mme Morin: Nous avons une préférence au Canada. Nous avons une loi qui protège la vie privée — on en a parlé la semaine passée — qui est la Loi sur la protection des renseignements personnels et les documents électroniques. Cette loi exige le consentement de l'intéressé pour qu'on puisse utiliser ses renseignements personnels. Une adresse électronique est dans la plupart des cas un renseignement personnel. La forme que doit revêtir le consentement dépend du contexte et aussi de l'importance de l'information. Je pense qu'on peut facilement dire que la plupart des gens conviendraient que leur adresse électronique est un renseignement personnel relativement important précisément à cause du problème des pourriels. Il y a 10 ans, lorsque les premiers courriels ont commencé à être envoyés, ce n'aurait peut-être pas été le cas parce que, à l'époque, si je ne recevais que cinq courriels, j'imagine qu'en recevoir un de plus ne m'aurait pas vraiment dérangé. Mais aujourd'hui, les attentes sont très différentes, non seulement en ce qui concerne l'utilisation du courriel, mais également pour ce qui est des messageries instantanées ou des messages qui vous parviennent par votre téléphone mobile. Les gens veulent pouvoir donner leur autorisation avant de recevoir ce genre de messages, d'où la formule de l'acceptation expresse. C'est pour l'essentiel ce qu'utilisent ici au Canada ceux qui veulent vraiment honorer ce genre de demande. Aux États-Unis, la formule du refus est en usage depuis de nombreuses années, non pas seulement en ce qui concerne les pourriels et le courriel, mais pour tout ce qui touche à la protection de la vie privée en général. Si les Américains ont privilégié la formule du refus, cela s'explique par la façon générale dont ils protègent la vie privée, préférant partir du principe qu'il y a consentement jusqu'à preuve du contraire, de sorte qu'ils ont procédé de la même façon pour le courrier électronique.

Les États-Unis sont également à l'origine de la moitié des pourriels envoyés dans le monde entier. Il y a de l'argent à gagner dans ce domaine. Il est évident que ces gens payent quelqu'un. Il y

e-mail. It is a different approach. Their federal law was passed to take precedence over stricter state laws. In California, they had a bill that came into force on January 1, but the federal law has usurped that provision, which was an opt-in approach to e-mail. We have privacy legislation that, in essence, has brought us to an opt-in approach when it comes to the use of e-mails. I think we prefer that approach.

Senator Merchant: Who owns the right to access the electronic media market? Can you buy the airwaves? Do you know what I am trying to say?

Mr. Thomson: It is a very interesting question, particularly as it relates to the Internet, which is a worldwide medium developed for the free exchange of information, without borders or controls in most cases, unless you as an end-user want to put controls on what you receive. I would suggest that Internet experts and those who are interested in Internet policy would say that everybody owns the Internet.

Senator Merchant: I have a question. To what extent should regulations protect people from unwanted messages and advertising, although they may have validity? How do we distinguish those ads and messages from those for which you are paid but which are also unwanted? Is it not accurate to say that almost all advertisements and messages in electronic media are unwanted, although we benefit from some advertisements? What is the qualitative difference between those advertisements that hosted under your organization and those that are not? You may set standards, but is not the greatest concern about who profits from these standards?

Ms. Morin: To begin with, there is a great difference in the kinds of advertising messages you receive via e-mail. In the case of Bell Canada's marketing messages to customers, we sought and received their okay because they opted in on-line by ticking a box that says, "Please send me more information on new products and services." That question is being asked and positive replies are added to your distribution list. Every e-mail containing marketing material sent to customers has an unsubscribe box at the bottom, which is respected. Some customers may unsubscribe or may re-subscribe. That is a specific incidence of a customer requesting material. Air Canada's Web site is used as a very good Canadian example of a success story when it comes to marketing. They e-mail marketing materials only to those who have opted in. Every Wednesday, the customer will receive the promotional material from Air Canada on the specials for the weekend. It has been a highly successful campaign.

Then there are the truly unwanted ads, for items such as medications, get-rich schemes and other fraudulent schemes. In the middle is the grey zone, of individuals who might receive an e-

a davantage de cibles et aussi davantage de gens à qui envoyer des courriels. Les États-Unis ont une loi fédérale qui prime sur certaines lois plus rigoureuses adoptées dans certains États. En Californie, une proposition de loi est entrée en vigueur le 1er janvier, mais la loi fédérale a invalidé cette disposition qui prévoyait, dans le cas du courrier électronique, une formule d'acceptation expresse. Au Canada, nous avons une loi qui protège la vie privée et qui a tout naturellement fait que nous avons opté pour la formule de l'acceptation expresse dans le cas du courrier électronique. Je pense que nous préférons ce genre de formule.

Le sénateur Merchant: À qui appartient le droit d'accès au marché des médias électroniques? Est-ce qu'on peut acheter des ondes hertziennes? Comprenez-vous ce que je veux dire?

M. Thomson: C'est une question intéressante, en particulier dans le contexte d'Internet, ce médium planétaire permettant d'échanger gratuitement de l'information, sans frontières ou sans contrôles dans la plupart des cas, à moins que l'utilisateur souhaite exercer un contrôle sur ce qu'il reçoit. Je suppose que les spécialistes d'Internet et ceux qui s'intéressent à la politique d'Internet vous diraient qu'Internet appartient à tout le monde.

Le sénateur Merchant: J'ai une question. Dans quelle mesure la réglementation devrait-elle protéger les particuliers des messages et de la publicité non désirés, quelle qu'en soit la validité? Comment distinguer ces messages et annonces de ceux pour lesquels vous êtes payés mais qui sont aussi non désirés? N'est-il pas exact de dire que presque tous les messages et annonces dans les médias électroniques sont non désirés, même si nous profitons de certains? Quelle différence de qualité y a-t-il entre les messages publicitaires dont s'occupe votre organisme et les autres? Vous fixez peut-être des normes, mais ne convient-il pas de se préoccuper avant tout de savoir qui profite de ces normes?

Mme Morin: Pour commencer, il y a une différence considérable entre les différentes formes de messages publicitaires qu'on reçoit par courriel. Dans le cas des messages commerciaux de Bell Canada à ses clients, nous sollicitons et recevons leur accord qu'ils expriment en direct en cliquant sur une fenêtre portant l'indication «Envoyez-moi de l'information sur les nouveaux produits et services, s'il vous plaît». Les réponses positives sont ajoutées à la liste de distribution. Tout courriel contenant de l'information commerciale et qui est envoyé aux clients comporte au bas de l'écran une fenêtre de non-abonnement, qui est respectée. Les clients peuvent refuser l'abonnement ou se réabonner. Vous avez ici le cas particulier d'un client qui demande de l'information. Le site Web d'Air Canada est un excellent exemple canadien de réussite en matière commerciale. Il n'envoie de l'information commerciale qu'à ceux qui en demandent. Tous les mercredis, le client reçoit une offre promotionnelle d'Air Canada annonçant les tarifs spéciaux de la fin de semaine. C'est une campagne très efficace.

Il y a ensuite des annonces véritablement non désirées, pour des produits comme des médicaments, des combines pour devenir riche et autres manoeuvres frauduleuses. Entre les deux, on trouve

mail from an organization with which they do not have an existing relationship but in which they might be interested. In such a case, it results in a positive ad message.

That kind of activity keeps the spammers in business, in a way. I think Senator Oliver alluded to the figure of 0.0001 per cent, because the spammers do not have to pay to send their e-mail out — they pay for their Internet connection only — and so they are banking on getting a handful of people, out of millions, who will actually click through to the ad.

One of the campaigns started last fall was, "Do not reply and do not buy." If it is something that you have not asked for, just delete it to eliminate the business model. That sends a message back to the spammers and they may have to move to a different business model as a result. It is because there is no cost to send the e-mail that they can take the chance of sending it to everyone.

There is a difference in the kind of advertising material that people receive: requested, non-requested and unwanted, and non-requested and wanted.

Mr. Thomson: With respect to spam, the only one who profits is the spammer. Everyone else pays the cost, including the ISPs and end-users. There is no profit motive for ISPs or end-users with respect to spam and it is a cost that they wish to avoid.

Senator LaPierre: I do not know what all the fuss is about, because life is full of risks. My newspaper — the *Ottawa Citizen* — comes every day and is full of junk that I do not want. It sells me everything from the bathtub to the kitchen sink. I do not need it and I do not want it. No one is appearing before this committee to say that we must control the *Ottawa Citizen* so they do not send junk messages to people.

The Web is the last area of freedom in the world into which the bureaucrats and politicians have not put their filthy noses. We are now in the process of attempting to control the Web. In controlling the Web, we will destroy it as an instrument of communication. Consequently, I thank you for appearing before us to bring some sanity to this discussion. That is all I have to say.

Mr. Thomson: Thank you, senator.

Senator Day: I do not know if I dare say that I find some of the proposed legislation from Senator Oliver rather interesting.

In respect of the statistics, I would like to get my mind around this issue a little better. We talked last time with Senator Oliver about this. According to the statistics that I read, about 90 per cent of what we describe as unsolicited spam originates outside Canada. Could you confirm that figure?

Mr. Thomson: That is our understanding as well.

Senator Day: About 50 per cent of everything end-users receive is unsolicited and unwanted material. Is the figure that high?

Mr. Thomson: It is that and more — up to 60 per cent and more. Over the Christmas season it can be as high as 75 per cent.

une zone grise, où l'internaute peut recevoir un courriel d'un organisme avec lequel il n'a pas de relation mais auquel il est susceptible de s'intéresser. Dans ce cas, on obtient un message publicitaire positif.

Voilà le genre d'activité qui occupe les polluposteurs. Le sénateur Oliver a annoncé, je crois, le chiffre de 0,0001 p. 100, parce que ces derniers n'ont pas à payer pour envoyer leur courriel; ils ne paient que pour leur abonnement Internet, et ils espèrent seulement attraper quelques personnes sur des millions, qui vont cliquer pour voir leur annonce.

L'une des campagnes lancées l'automne dernier a pour slogan «ne répondez pas et n'achetez pas». Si on vous propose quelque chose que vous n'avez pas demandé, il faut le supprimer pour éliminer ce modèle commercial. Vous renvoyez ainsi un message aux polluposteurs qui risquent de devoir changer de modèle commercial. C'est parce que l'envoi d'un courriel ne coûte rien qu'ils peuvent prendre le risque d'en envoyer un à tout le monde.

Il y a des différences dans le genre de messages publicitaires que reçoivent les internautes: le message peut être demandé, non demandé et non souhaité, et non demandé et souhaité.

M. Thomson: En ce qui concerne le pourriel, le seul qui en profite est le polluposteur. Tous les autres paient quelque chose, y compris les fournisseurs de services Internet et les utilisateurs, auxquels le pourriel ne peut apporter aucun profit; c'est par contre un coût qu'ils souhaitent éviter.

Le sénateur LaPierre: Je ne sais pas pourquoi on en fait tout un foin, car la vie est pleine de risques. Mon journal, le *Ottawa Citizen* est rempli tous les jours d'annonces publicitaires dont je n'ai cure. On veut tout me vendre, de la baignoire à l'évier de cuisine. Je n'en ai pas besoin et je n'en veux pas. Personne ne comparaît devant notre comité pour dire qu'il faut contrôler l'*Ottawa Citizen* pour l'empêcher d'envoyer ces messages inutiles.

Le Web est le dernier îlot de liberté au monde dans lequel les fonctionnaires et les politiciens n'ont pas encore fourré leur nez. Nous sommes en train d'essayer de le contrôler. En contrôlant le Web, nous allons détruire cet instrument de communication. Par conséquent, je vous remercie de comparaître devant nous pour apporter un peu de bon sens au débat. C'est tout ce que j'ai à dire.

M. Thomson: Merci, sénateur.

Le sénateur Day: C'est à peine si j'ose le dire, mais je trouve le projet de loi du sénateur Oliver assez intéressant.

J'aimerais améliorer ma compréhension des statistiques. Nous en avons parlé la dernière fois avec le sénateur Oliver. D'après les statistiques dont j'ai eu connaissance, 90 p. 100 environ de ce que l'on qualifie de pourriels non sollicités provient de l'étranger. Pouvez-vous confirmer ce chiffre?

M. Thomson: Oui.

Le sénateur Day: À peu près la moitié de tout ce que reçoivent les internautes est non sollicité et non souhaité. Est-ce bien cette proportion?

M. Thomson: C'est plus que cela: 60 p. 100 et plus. Dans le temps des Fêtes, elle peut atteindre 75 p. 100.

Senator Day: Senator LaPierre's newspaper would have to be 75 per cent advertising for fridges and stoves to be comparable.

Ms. Morin: He would have to receive, with his daily paper, a truckload of unwanted advertising.

Senator LaPierre: The principle is that we consider spam to be someone else's information, and therefore someone else's cross to bear. We are talking about unsolicited and unwanted information of any kind. Whether or not I receive three pages in the daily paper that tell me what I should buy and how to buy it, there is always a supplement in magnificent colour. The same thing occurs on the Web. Whether it is 10,000 pages or one page, it is too many. However, if I were to control the Web, then I would have to control the newspaper as well, through legislation. That is my point, and the Web continues to be the only area of freedom that we have and we must not endanger that.

Senator Day: Following along with my line of questioning, you indicated that one of the approaches to control is through existing legislation, which would be the Competition Act. We reviewed these before, and Mr. Thomson mentioned privacy legislation, personal information legislation and the Criminal Code in certain instances. If that were a feasible approach to this issue, or part of this multi-faceted approach, what would you see as commencing these legal actions?

Ms. Morin: If it fell under the Criminal Code, we would expect to see the RCMP and other police agencies involved. Depending on the different provisions and offences, there could injunctions issued and fines paid.

If you turn to the provisions of the Competition Act on fraudulent and misleading advertising, it would be the Competition Bureau that could launch these prosecutions, whether on the criminal or civil side.

Under privacy legislation, it can be through several different ways. It could be an individual who files a complaint with the Office of the Privacy Commissioner, saying, "I am receiving this information. I have asked them to take my e-mail address off their list and I continue to receive information from them." That would be a privacy complaint, just as in any other context.

Something that is not well understood about the privacy legislation that now applies across the country — except B.C., Alberta and Quebec have their own legislation, but it is similar — is once you have a finding from the Privacy Commissioner, you can go to the Federal Court for a new trial. If in fact there is breach of the act, you can have the Federal Court judge issue just about anything — whether it is an injunction prohibiting them from engaging in these activities or from even having an Internet access, whatever the judge might find suitable, including punitive damages. It is explicit in the legislation that you can seek punitive damages. Many of the spammers — and this would apply to Canadian spammers who engage in this activity — could be required to pay hefty fines.

Le sénateur Day: Pour faire la comparaison, il faudrait que le journal du sénateur LaPierre contienne 75 p. 100 de publicité pour les réfrigérateurs et les cuisinières.

Mme Morin: Il faudrait qu'il reçoive, avec son journal quotidien, un plein camion de publicité non souhaitée.

Le sénateur LaPierre: Nous considérons que le pourriel est de l'information destinée à quelqu'un d'autre, qui devra donc en faire les frais. On peut aussi parler de toutes les formes d'information non sollicitées et non souhaitées. Que je reçoive ou non, dans mon journal, trois pages où on va me dire ce que je devrais acheter, il y a toujours un supplément aux couleurs magnifiques. C'est la même chose sur le Web. Que ce soit une page ou 10 000, c'est toujours trop. Mais si on contrôle le Web, il faudrait aussi contrôler les journaux par voie législative. Voilà ce que je veux dire, et le Web reste le seul îlot de liberté que nous ayons, et il ne faut pas menacer cette liberté.

Le sénateur Day: Pour reprendre le thème de mes questions, vous avez dit qu'on pourrait exercer ce contrôle grâce à la législation actuelle, en l'occurrence la Loi sur la concurrence. Nous avons déjà abordé ce thème, et M. Thomson a dit que dans certains cas, il faudrait aussi recourir à la législation sur la protection de la vie privée et des renseignements personnels, et au Code criminel. Si c'est une façon d'aborder le problème, et même s'il y en a d'autres, comment pensez-vous qu'on puisse intenter des poursuites?

Mme Morin: Si on constate une infraction prévue au Code criminel, on devrait s'attendre à ce que la GRC ou un autre service de police intervienne. Selon les dispositions invoquées ou le type d'infraction, des injonctions pourraient être émises et des amendes imposées.

En ce qui concerne les dispositions de la Loi sur la concurrence concernant la publicité trompeuse et frauduleuse, le Bureau de la concurrence pourrait intenter des poursuites au civil ou au pénal.

La législation sur la protection de la vie privée peut être invoquée de différentes manières. Il peut s'agir d'un particulier qui porte plainte auprès du Bureau du commissaire à la vie privée en disant: «Je reçois cette information. J'ai demandé que l'on supprime mon adresse de la liste de distribution et on continue à me l'envoyer.» Ce serait une plainte en matière de vie privée, comme dans n'importe quel autre contexte.

Ce qu'on ne sait pas très bien sur la législation en matière de protection de la vie privée qui s'applique maintenant dans l'ensemble du pays — à l'exception de la Colombie-Britannique, de l'Alberta et du Québec, qui ont leur propre législation semblable à la loi fédérale — c'est qu'une fois qu'on a obtenu les conclusions du commissaire à la protection de la vie privée, on peut intenter un nouveau procès devant la Cour fédérale. En cas d'infraction à la loi, le juge de la Cour fédérale peut prendre toutes sortes de mesures, que ce soit une injonction interdisant les activités du polluposteur ou le privant d'accès à Internet, ou des dommages-intérêts exemplaires. La loi prévoit explicitement qu'on puisse demander des dommages-intérêts exemplaires. Les polluposteurs peuvent se voir imposer de lourdes amendes, et c'est aussi le cas des polluposteurs canadiens.

Senator Day: Who brings that private action? Is it the Internet service provider or the homeowner, the end-receiver of this information?

Ms. Morin: In this case, it would be the individual who is receiving the unwanted e-mail at home, or it could be an employee in an organization receiving unwanted e-mail. I know that ISPs would also be involved, because they would have to be able to prove to the Privacy Commissioner's office that the spammer was collecting the e-mail address through deceptive means. For example, had they asked to opt out? Therefore, an ISP might have a role to play. The Privacy Commissioner has the tools to consult different stakeholders in the chain to see if there are particular practices in place, or if there is evidence that they can provide.

The three pieces of legislation together will come very close, if enforced, to sending a signal to spammers that this will not be tolerated.

Senator Day: As Internet service providers, although you might be indirectly involved in one of these actions, when you say Canada is not missing anti-spam laws and what we are missing is the targeted and aggressive enforcement of those laws — and that was your comment, Mr. Thomson — you are really saying that somebody else is not enforcing existing laws. The government is not enforcing them.

Mr. Thomson: That is correct.

Senator Day: Ms. Morin outlined another issue that is important for us to keep in mind. National laws do not reach outside the country, and 90 per cent of the spam is coming from somewhere else. It makes it very difficult for Canadian laws to deal with the people outside the country who are sending this material on the Internet — because it is an international business. Do you agree with that?

Mr. Thomson: Very much so.

Senator Day: What are you doing in your discussions with other associations in other countries around the world? Can you explain what is going on in terms of international cooperation? Are you leaving that to the same government department that has not come forward with an action plan?

Mr. Thomson: As an ISP association, CAIP has membership in a loose group of other ISP associations around the world. It regularly exchanges information, ideas and so on with the staff of other ISP associations. There are existing relationships.

In fact, a year ago, CAIP worked with the Australian Internet service provider industry on this public awareness campaign that Ms. Morin mentioned before — the "Don't buy, don't reply, don't try" regime. There is cooperation and communication on the ISP association-to-association level, and there is also increasing cooperation among ISPs themselves, both domestically and internationally. Perhaps Ms. Morin can talk about that.

Le sénateur Day: Qui peut intenter cette action? Le fournisseur de services Internet ou le particulier qui reçoit cette information?

Mme Morin: En l'occurrence, c'est celui qui reçoit le courriel non souhaité chez lui, ou un employé d'un organisme qui reçoit ce courriel non souhaité. Je sais que les fournisseurs Internet peuvent aussi intervenir, car ils sont en mesure de prouver au commissaire à la protection de la vie privée que le polluposteur a obtenu l'adresse électronique par des moyens déloyaux. Par exemple, le fournisseur a pu demander à se faire retirer de la liste de distribution. Il peut donc avoir un rôle à jouer. Le commissaire à la protection de la vie privée a les outils nécessaires pour consulter différents intervenants dans la chaîne pour vérifier les pratiques ou pour demander des preuves.

En appliquant ces trois mesures législatives, on peut pratiquement signaler aux polluposteurs que leur activité ne sera plus tolérée.

Le sénateur Day: En tant que fournisseurs de services Internet, même si vous pouvez intervenir indirectement dans des poursuites, lorsque vous dites que le Canada ne manque pas de lois antipourriels et que ce qui fait défaut, c'est une mise en oeuvre ciblée et agressive de la législation — c'est ce que vous avez dit, monsieur Thomson — vous voulez dire en réalité que quelqu'un d'autre n'applique pas la législation en vigueur. Le gouvernement ne l'applique pas.

M. Thomson: C'est exact.

Le sénateur Day: Mme Morin a soulevé une autre question qu'il importe de garder à l'esprit. La législation nationale ne s'applique pas à l'étranger. Or, 90 p. 100 du pourriel vient de l'étranger. Il est donc très difficile d'invoquer la législation canadienne contre des polluposteurs à l'extérieur du pays qui envoient leurs messages sur Internet, car il s'agit d'activités internationales. Est-ce aussi votre avis?

M. Thomson: Tout à fait.

Le sénateur Day: Quelle est la teneur de vos discussions avec vos homologues étrangers? Pouvez-vous nous parler de la coopération internationale? Est-ce que vous vous en remettez à ce même ministère qui n'a pas présenté de plan d'action?

M. Thomson: En tant qu'association de fournisseurs Internet, l'ACFI est membre d'un groupe informel d'associations de fournisseurs de services Internet de différents pays. Nous échangeons régulièrement de l'information et des idées avec le personnel des autres associations. Ces relations existent.

Il y a un an, l'ACFI a collaboré avec les fournisseurs Internet australiens dans le cadre de la campagne de sensibilisation évoquée par Mme Morin, où l'on disait: «N'achetez pas, ne répondez pas, n'essayez pas.» Il y a coopération et communication entre les associations de fournisseurs et entre les fournisseurs eux-mêmes, aussi bien au Canada qu'au niveau international. Mme Morin pourrait peut-être vous en parler.

Ms. Morin: It has taken some time, but Mr. Thomson is correct, ISPs have sought each other out. Not just through the association, but also for self-preservation, they have sought out ISPs from which, for example, spam is coming, or to which perhaps some of their customers are spamming. We are trying to keep spam from leaving our network, and vice versa. I know Bell Canada, TELUS and other Canadian ISPs are now part of this group of North American ISPs that deal with each other. We have contact information; we are sharing best practices, filtering techniques and different benchmarks for what we will or will not allow on our networks. We are seeing a new rise in spam, using viruses to propagate it. How do we help our customers out? We are using that kind of association, at a loose level, to make that happen.

At the international level, you need to get the players speaking to each other, but you also need to get ISPs speaking with other government agencies from around the world. Then you need to get the agencies from around the world speaking to each other. You need international cooperation at multiple levels. We need agencies in Canada speaking to each other, and that is why we have this new campaign on enforcement of existing laws — trying to get the various agencies together with the industry players that can help; we need to get them speaking to their counterparts, and that is happening. Industry Canada has been active internationally, at the OECD and other places. Whether through private sector organizations like the Global Business Dialogue on Electronic Commerce that was referred to before — the GBDe — we have brought industry players and government together to educate people. It has taken a long time to have people understand the impact it is having on the different players.

Many people allude to the cyber-crime treaty that different countries are moving to implement. That is another tool available to countries to pursue the illegal and fraudulent nature of spam.

Senator Day: That is helpful. Just so I understand the information you are giving us here, your recommended approach is one of international cooperation. You talk about new technologies, about enforcement of existing laws; and you do not see the necessity, at this stage, for any new laws in relation to this problem.

Ms. Morin: Not at this stage.

Senator Day: You also talked about self-regulation. That is the multi-faceted approach. Can you talk a little about what you are doing from a self-regulatory point of view? Are you setting standards for all your members? What else are you doing?

Mr. Thomson: The starting point is that there is dialogue amongst CAIP members, which was initiated primarily by the Industry Canada paper that was issued a year ago. As a result, we created a task force within the association to look at how we

Mme Morin: Il a fallu un certain temps, mais M. Thomson a raison, les fournisseurs Internet ont pris contact entre eux, non seulement par l'intermédiaire de l'association, mais aussi pour se protéger, et ils ont recherché les fournisseurs d'où provenait le pourriel ou vers lesquels certains de leurs clients envoyaient du pourriel. Nous essayons d'empêcher le pourriel de sortir de nos réseaux, et vice versa. Je sais que Bell Canada, TELUS et d'autres fournisseurs canadiens font partie d'un groupe de fournisseurs nord-américains qui sont en contact les uns avec les autres. Nous avons de l'information, nous partageons des pratiques exemplaires, des techniques de filtrage et différents points de repère concernant ce que nous n'acceptons pas sur nos réseaux. On assiste actuellement à une montée des pourriels qui utilisent des virus pour se propager. Comment pouvons-nous aider nos clients? Nous nous servons des associations informelles pour y parvenir.

Au niveau international, il faut que les intervenants communiquent entre eux, mais il faut aussi que les fournisseurs Internet s'adressent aux autorités gouvernementales. Il faut aussi que les organismes gouvernementaux du monde entier communiquent entre elles. Il faut assurer la coopération internationale à plusieurs niveaux. Il faut que les organismes canadiens se parlent entre elles, et c'est pourquoi nous avons entrepris cette campagne qui demande l'application des lois existantes — nous essayons de faire intervenir les différents organismes et les intervenants de l'industrie qui peuvent agir; nous devons les amener à prendre contact avec leurs homologues étrangers, et c'est effectivement ce qui se produit. Industrie Canada agit au niveau international, à l'OCDE et dans d'autres tribunes. Par l'intermédiaire d'organismes privés comme Global Business Dialogue on Electronic Commerce, dont il a été question tout à l'heure, nous avons réuni des entreprises et des organismes gouvernementaux pour faire de l'éducation. Il a fallu un certain temps pour faire comprendre l'impact du pourriel sur les différents intervenants.

On entend souvent parler du traité sur la cybercriminalité que différents pays s'apprêtent à mettre en oeuvre. C'est un autre outil qui permet de faire échec au caractère illégal et frauduleux du pourriel.

Le sénateur Day: C'est très utile. J'aimerais m'assurer de bien comprendre l'information que vous nous livrez. La formule que vous préconisez est celle de la coopération internationale. Vous parlez des nouvelles technologies, de l'application de la législation en vigueur et vous ne voyez pas la nécessité, dans le contexte actuel, d'adopter de nouvelles lois pour régler ce problème.

Mme Morin: Pas dans le contexte actuel.

Le sénateur Day: Vous avez aussi parlé d'autoréglementation. C'est l'approche sur plusieurs fronts. Pouvez-vous nous parler un peu de ce que vous faites en matière d'autoréglementation? Est-ce que vous fixez des normes pour tous vos membres? Que faites-vous d'autre?

M. Thomson: Au point de départ, il y a ce dialogue entre les membres de l'ACFI, qui s'est amorcé essentiellement autour du document publié il y a un an par Industrie Canada. Nous avons créé au sein de l'association un groupe de travail qui élabore notre

would respond to that particular paper. Flowing from that was movement toward developing a code of conduct or a best-practices approach within the association, among its members, to deal with issues like open relays, how to respond to customer complaints and so on.

That was taking place before I left the association in February. The association has been in a transition stage since that time, so there has been a bit of a hiatus with respect to those activities. However, I am confident they will be starting up again in the near future as the organization is ready to move forward again under new leadership.

Senator Day: Do you have full-time people? Would this have been a part-time volunteer position that you held?

Mr. Thomson: I was a full-time employee. Currently, there is no person in my role, but there will be in due course.

Senator Day: Do you wish to add anything, Ms. Morin?

Ms. Morin: There is a fifth tool, and that is awareness and education.

Again, we need user awareness and education on how to protect their systems, because the spammers are beginning to use their computers to send out spam to others; how to not give out your e-mail address at just any Web site, as you would not give out your name and address to somebody you met on the street.

There is education of ISPs. The ISPs in Canada — and we are working with the cable ISPs — are coming together because, for example, it is in my corporate best interests that other ISPs do not allow spam from their networks to enter my network, just as it is in their best interests that I control the customers on my network who may want to send spam. We are helping to raise the bar and develop best practices there.

There is also education of government and different government agencies about the role they can play, the impact on ISPs, and the value of filtering technologies, for example. We referred earlier to the expert workshop held here in Ottawa in June. We had in attendance the Organization for Economic Cooperation and Development, OECD; Industry Canada; different ISP associations and ISPs; and marketing associations. Some marketers are finding that their e-mail is not getting through. The filters are blocking it, what is called the false positives. They were pushing hard for the ISPs to stop filtering, saying that the filter should only be active further into the network, at the user level. We can understand their frustration, but given the small margin of error, if ISPs were to stop filtering tomorrow, you would not get any e-mail. The Internet would grind to a halt because of the volume of e-mail out there. No e-mail would get through to anybody. The filtering has to continue. It has to become better. We need the white list. We need different tools, like sender authentication, so I can prove the e-mail is coming from Senator Day, for example, and I will let that one in, but if someone is faking where the e-mail is coming from, I will

réponse à ce document. À partir de là, on s'est efforcé d'élaborer un code de conduite ou un recueil de pratiques exemplaires parmi les membres de l'association, pour traiter de questions comme les relais ouverts, la façon de répondre aux plaintes des consommateurs, et cetera.

Je parle ici de ce qui s'est passé avant que je quitte l'association en février. Depuis lors, elle est entrée dans une phase de transition, et ses activités ont été plus ou moins interrompues, mais je suis certain qu'elles vont reprendre dans un proche avenir car l'organisme est prêt à repartir de l'avant avec de nouveaux dirigeants.

Le sénateur Day: Est-ce que vous avez des employés à plein temps? Votre poste était-il bénévole et à temps partiel.

M. Thomson: J'étais employé à plein temps. Actuellement, le poste est vacant, mais il devrait être doté tôt ou tard.

Le sénateur Day: Voulez-vous ajouter quelque chose, madame Morin?

Mme Morin: Il y a un cinquième outil, c'est la sensibilisation et l'éducation.

Il faut sensibiliser les utilisateurs et leur apprendre à protéger leurs systèmes, parce que les polluposteurs commencent à utiliser les ordinateurs des internautes pour propager leurs messages; les internautes doivent savoir qu'ils ne doivent pas donner leur adresse électronique à n'importe quel site Web, de la même façon qu'on ne donne pas son nom ni son adresse à n'importe qui dans la rue.

Il faut aussi faire l'éducation des fournisseurs Internet. Les fournisseurs canadiens — et nous travaillons avec les fournisseurs par câble — collaborent parce que, par exemple, j'ai intérêt à ce que les autres fournisseurs ne laissent pas sortir de leur réseau du pourriel qui va pénétrer dans le mien, et ils ont un même intérêt à ce que je contrôle les clients de mon réseau qui voudraient envoyer du pourriel. Nous nous efforçons tous d'élever la barre et d'adopter des pratiques exemplaires.

Il faut aussi faire l'éducation du gouvernement et des différents organismes gouvernementaux quant au rôle qu'ils peuvent jouer, aux conséquences de leur action sur les fournisseurs et la valeur des technologies de filtrage, par exemple. Nous avons parlé tout à l'heure de l'atelier qui s'est tenu à Ottawa en juin dernier. Il a réuni des représentants de l'OCDE, d'Industrie Canada, des différentes associations de fournisseurs, des fournisseurs et des associations commerciales. Certains commerçants constatent que leur courriel n'atteint pas ses destinataires et qu'il est bloqué par des filtres; c'est ce qu'on appelle de faux positifs. Ils ont fait pression auprès des fournisseurs pour qu'ils cessent le filtrage, disant que le filtre devrait intervenir à la périphérie du réseau, au niveau des utilisateurs. Nous comprenons leurs doléances, mais compte tenu de la faible marge d'erreur, si les fournisseurs cessaient le filtrage, personne ne recevrait plus de courriels. Le réseau Internet serait paralysé à cause du volume du courriel. Personne ne pourrait plus recevoir de messages. Le filtrage doit continuer. Il s'est déjà amélioré. Nous avons besoin de la liste blanche et de différents outils, comme l'authentification de l'expéditeur, qui me permet de prouver, par exemple, que ce

put it to the side and not let it in. These are the standards the ISPs are working on. It is truly an international issue, so that we, as an ISP, cannot just say, "This is what I am going to do." We need to work together, and by default, that will take some time. People are talking to each other and we have made great strides; mind you, so have the spammers.

Senator Day: If all the ISPs were not cooperating on this, when one gets blocked, it would find another way to get to where it is going.

Ms. Morin: That may happen.

Senator Day: Everyone has to be into this, on an international level.

Ms. Morin: Yes.

The Chairman: My questions come from a state of near-perfect ignorance. I am a technological klutz, but the questions have to do with money. You were outlining citizens' possible recourse to the courts, but it is an enormously expensive process for the individual to undertake. It is more likely to be an individual than a corporation having terrible problems, because if worst comes to worst, the corporation can employ somebody full time to delete the spam. It is the individual whose whole day can be absorbed by removing this.

Why should the onus be on individuals to protect themselves from spam, perhaps at great cost? This is something of a devil's advocate question, but it is a real one. Why should there not be a role for the state in saying there are limits beyond which you cannot go in abusing the privacy of individuals, and then act on it?

Ms. Morin: In a sense, that is exactly the point. The privacy legislation allows an individual to complain to the Privacy Commissioner, whether at the provincial or federal level. We are not hoping there will be thousands of people complaining to the Office of the Privacy Commissioner about spam because they will not be able to deal with the flood of investigations they will have to conduct. Just as in any litigation model, whether under the Criminal Code, the Competition Act or the privacy legislation, you would like to see one or two examples of enforcement. Someone has either gone to jail, had to pay a hefty fine or has been precluded from continuing activities; and the federal Privacy Commissioner has the ability, with the consent of the individual, to take the action to the Federal Court.

The Chairman: I understood you to say that the individual had to do it. The commissioner can do it?

Ms. Morin: The individual must be the one who complains, but after that, it is the commissioner.

The Chairman: I have a second money question, again based on complete technological illiteracy, and it concerns your statement that spammers have no cost, apart from the basic subscription fee.

courriel provient du sénateur Day et que je peux le laisser passer, mais si quelqu'un essaie de falsifier l'origine d'un courriel, je ne le laisserai pas passer. Voilà les normes sur lesquelles les fournisseurs travaillent. C'est vraiment une question internationale et chaque fournisseur ne peut pas agir en vase clos. Tout le monde doit travailler ensemble, ce qui va prendre un certain temps. Les intervenants communiquent entre eux et nous avons fait des progrès remarquables; évidemment, les polluposteurs aussi.

Le sénateur Day: Si tous les fournisseurs ne collaborent pas, un message bloqué trouvera une autre façon de se rendre à destination.

Mme Morin: C'est possible.

Le sénateur Day: Tout le monde doit participer au niveau international.

Mme Morin: Oui.

La présidente: Mes questions trahissent mon ignorance à peu près totale. Je suis un nul technologique, mais mes questions concernent l'argent. Vous avez parlé des recours devant les tribunaux, mais des poursuites sont très chères pour un particulier. Et le particulier risque plus d'avoir des problèmes qu'une société, car au pis aller, celle-ci peut employer quelqu'un à plein temps pour détruire les pourriels. En revanche, le particulier risque d'y passer la journée.

Pourquoi impose-t-on aux particuliers l'obligation de se protéger des pourriels, éventuellement à grands frais? Je me fais l'avocat du diable avec cette question, mais elle est bien réelle. Pourquoi l'État n'intervient-il pas en disant qu'il y a des limites au-delà desquelles il est interdit de porter atteinte à la vie privée?

Mme Morin: C'est précisément la question. La législation sur la protection de la vie privée permet à un particulier de porter plainte auprès du commissaire à la protection de la vie privée, au niveau provincial ou fédéral. Nous ne souhaitons pas que le Bureau du commissaire à la protection de la vie privée reçoive des milliers de plaintes sur le pourriel, car il serait incapable de faire face aux innombrables enquêtes qu'il devrait mener. Comme dans tout contentieux, que ce soit en vertu du Code criminel, de la Loi sur la concurrence ou de la législation sur la protection de la vie privée, il faudrait un ou deux exemples d'application de la loi. Il faudrait emprisonner un polluposteur, lui faire payer une lourde amende ou lui interdire de poursuivre ses activités. Et le commissaire fédéral à la protection de la vie privée peut, avec le consentement du plaignant, se pourvoir devant la cour fédérale.

La présidente: Vous dites, si je comprends bien, que c'est au particulier d'agir. Est-ce que le commissaire peut agir de sa propre initiative?

Mme Morin: Le particulier doit porter plainte, mais après cela, c'est au commissaire d'agir.

La présidente: J'ai une deuxième question d'argent, qui prouve elle aussi ma complète ignorance en matière technologique; vous dites que les polluposteurs n'ont rien à payer, à part leur

The reason Senator LaPierre does not get a truckload of flyers with his newspaper every day is that the advertiser has to pay to include the material with the newspaper. There is quite an efficient self-regulating market system there, if you will, that keeps the volume down to manageable proportions. Nothing is perfect, because if the computer is in Fiji it is harder to control, but let us talk about Canadian spammers — why cannot Canadian ISPs start levying charges on people who are clearly sending out these huge volumes of unwanted messages?

Mr. Thomson: The starting point would be, rather than charging that customer, the ISP will in fact enforce their contract, which says "You shall not use our network to spam," and cut that customer off.

The money issue has been debated for some time now within the Internet community. The question is how can one equate, in an economic sense, e-mail messaging with the postal service? Is there a way, within this medium that has developed over the years as a free exchange of information, to introduce an obligation to pay a "stamp" charge on an e-mail message? It would be a fundamental rewrite of the whole Internet system. I think it is beyond any of our capabilities at this point. Nevertheless, there are ongoing studies and research into how one can change the economics of e-mail.

The Chairman: I am talking about the bulk material, not me dealing with Aunt Minnie.

Ms. Morin: To begin with, even though ISPs are trying to filter out the bulk spam, the spammers are also becoming smarter. They know that ISPs are setting different benchmarks at which they will terminate their service. A year ago, that benchmark might have been 100,000 e-mails. If there were 100,000 e-mails coming out of somewhere, we knew something was wrong so we either suspended or terminated the service. That individual might have gone somewhere else or tried to open another account, so we try to make sure we know with whom we are dealing.

They are smarter. They send them out 1,000 at a time. Or they hijack your computers while they are on-line; it will spit out 10, 100, 1,000 e-mails and then it will stop.

While the notion of putting a charge on the spammer has a lot of appeal, trying to come up with that kind of mechanism in today's framework is not easy; people are not used to having to pay to receive or send e-mail.

We find ourselves in a difficult situation because of these viruses. We know we have residential customers whose computers are sending out nasty spam to AOL customers elsewhere. We know that they do not know it is happening. We are wondering, as a business, how do deal with these customers. Should we get in touch with the customers and hand-hold them through this? If we turn it around and say we would have to charge that individual

abonnement Internet. Si le sénateur LaPierre ne reçoit pas un plein camion de dépliants publicitaires avec son journal quotidien, c'est que les annonceurs doivent payer pour les faire insérer dans le journal. C'est un système très efficace d'autoréglementation du marché, si l'on veut, qui maintient le volume de la publicité dans des proportions gérables. Rien n'est parfait, car si l'ordinateur se trouve aux Îles Fidji, le contrôle sera plus difficile, mais parlons des polluposteurs canadiens: pourquoi un fournisseur canadien de services Internet ne pourrait-il pas commencer à imposer des frais à ceux qui envoient d'énormes volumes de messages non souhaités?

M. Thomson: Au lieu d'imposer des frais à ce client, le fournisseur Internet pourrait commencer par invoquer les dispositions du contrat qui disent: «Il est interdit d'utiliser notre réseau pour envoyer du pourriel», et interrompre l'abonnement de ce client.

Dans la communauté Internet, on débat depuis un certain temps de la question d'argent. Il s'agit de savoir si, au plan économique, on peut assimiler un message électronique à un service postal. Dans le contexte de ce médium qui s'est développé au fil des années en tant que moyen gratuit d'échange d'informations, y aurait-il moyen d'imposer l'obligation d'acquitter des frais d'affranchissement sur chaque message électronique? Ce serait une remise en cause fondamentale de toute la formule Internet. Je pense que nous n'en avons pas les moyens actuellement. Néanmoins, on continue d'étudier la façon dont on pourrait modifier l'économie du courrier électronique.

La présidente: Je parle des envois collectifs, et non pas de tante Minnie.

Mme Morin: Pour commencer, même si les fournisseurs s'efforcent de filtrer les envois collectifs de pourriels, les polluposteurs raffinent eux aussi leurs méthodes. Ils savent que les fournisseurs mettent en place différents points de repère au-delà desquels ils interrompent leur service. Il y a un an, le point de repère était peut-être de 100 000 messages. Lorsque 100 000 messages arrivaient, nous savions qu'il y avait un problème et nous pouvions suspendre temporairement ou définitivement le service. Par la suite, le polluposteur a pu aller ailleurs ou essayer d'ouvrir un autre compte. Nous essayons donc de savoir à qui nous avons affaire.

Ils sont de plus en plus futés. Ils les envoient à raison de 1 000 à la fois, ou ils détournent votre ordinateur quand vous êtes connectés; l'ordinateur va envoyer 10, 100 ou 1 000 messages électroniques, puis il va s'arrêter.

L'idée d'imposer des frais au polluposteur est séduisante, mais il ne serait pas facile de l'imposer dans le contexte actuel. Les gens n'ont jamais eu à payer pour envoyer du courrier électronique ou pour en recevoir.

Nous sommes dans une situation difficile, à cause des virus. Nous avons des clients résidentiels dont les ordinateurs envoient du pourriel à des clients AOL ailleurs. Nous savons qu'ils l'ignorent. Comment agir avec ces clients? Est-ce qu'il faut entrer en contact avec eux et leur expliquer le phénomène? À l'inverse, si nous décidons d'imposer des frais de 2 cents par message envoyé, le système va s'effondrer rapidement, à cause de la façon dont les

customer the two cents per e-mail message sent, the model breaks down quickly because of how they do it. It is still discussed and batted around in technology industry circles. Some ISPs turn a blind eye to the fact that some of their customers are spamming because they are receiving their monthly fees. Eventually, the other ISPs receiving the spam will stop all mail from that one ISP. That is one way to exert pressure on ISPs to adopt best practices.

The Chairman: Go straight to the profit motive. I am a little less illiterate on that; and I thank you.

Senator Phalen: I take it from what I am hearing that you do not approve of Senator Oliver's bill?

Ms. Morin: Our position today is that we do not think Senator Oliver's bill is necessary at this time.

Senator Phalen: Other jurisdictions have addressed the problem of spam. Do they have legislation to cover that area?

Mr. Thomson: A number of jurisdictions have anti-spam legislation. We have talked about U.S. legislation, but there is also legislation in Korea and in a number of European countries; however, they are all different.

Senator Phalen: Is it effective?

Mr. Thomson: The amount of spam continues to increase, notwithstanding the anti-spam legislation in those jurisdictions. I would say that it has not proven effective yet.

Ms. Morin: We have noticed in the ongoing discussions and consultations that the expectation of a new law has caused some individual citizens to think that government will be able to legislate the problem away. That could have a backlash effect after raising individuals' expectations that a new law will make it go away.

Senator Phalen: We have laws, but we still have criminals. The question for me is, is the law necessary? Is it a fall-back position? Do you need a law to cover this area?

Ms. Morin: At this time, I do not think we do. We have not tried using the fraud provisions in the Criminal Code to see whether the RCMP could pursue those individuals, or the computer mischief provisions, whereby if someone tampers with your computer such that it hampers your enjoyment of the computer, or misleading advertising. It is definitely possible to capture some of the people who pay the spammers to get their marketing materials out. There is no doubt that those provisions could be used to go after that activity. The privacy legislation definitely has a role to play, to the extent that those activities are happening in Canada.

In a few years, we might say that we have tried the existing legislation route but it simply is not tight enough to cover this kind of activity. Spam is a tool being used to engage in criminal activity that is caught somewhere else. We might be back at it one day, but we have to try what is in place. When you compare the different legislation of other countries, short of adding new

polluposteurs procèdent. On continue à parler de ce problème dans le milieu des industries technologiques. Certains fournisseurs ferment les yeux sur leurs clients polluposteurs, car ils continuent à recevoir leurs abonnements mensuels. Les fournisseurs qui reçoivent du pourriel vont finir par bloquer tout le courrier de celui qui l'envoie. C'est une façon de faire pression sur les fournisseurs pour qu'ils adoptent des pratiques exemplaires.

La présidente: Allez directement à la recherche du profit. Je suis un peu moins ignorant en la matière; et je vous remercie.

Le sénateur Phalen: D'après ce que j'entends, vous n'êtes pas favorables au projet de loi du sénateur Oliver.

Mme Morin: Actuellement, nous ne pensons pas que le projet de loi du sénateur Oliver soit nécessaire.

Le sénateur Phalen: D'autres pays ont résolu le problème du pourriel. Est-ce qu'ils l'ont fait par la voie législative?

M. Thomson: Certains pays ont une législation antipourriels. Nous avons parlé de la loi américaine, mais il y a aussi une loi en Corée et dans certains pays d'Europe. Cependant, ces lois sont toutes différentes.

Le sénateur Phalen: Ces mesures sont-elles efficaces?

M. Thomson: Le volume du pourriel continue d'augmenter, malgré les législations antipourriels. Je dirais que l'intervention législative n'a pas encore prouvé son efficacité.

Mme Morin: Dans nos échanges avec nos partenaires, nous avons remarqué que la perspective d'une nouvelle loi avait amené certaines personnes à penser que le gouvernement pouvait régler le problème en légiférant. Il pourrait y avoir un retour de balancier, maintenant qu'on s'attend à ce qu'une nouvelle loi règle le problème.

Le sénateur Phalen: Nous avons des lois, mais nous avons toujours des criminels. Moi, je me demande si la loi est nécessaire. Est-ce que c'est une position de repli? Faut-il une loi dans ce domaine?

Mme Morin: Actuellement, je ne le pense pas. Nous avons essayé d'invoquer les dispositions du Code criminel en matière de fraude pour voir si la GRC ne pourrait pas poursuivre les polluposteurs, ou les dispositions sur les méfaits informatiques, qui interdisent d'altérer un ordinateur de façon que son propriétaire ne puisse plus s'en servir, ou bien encore les dispositions sur la publicité trompeuse. Il est certainement possible d'appréhender certains clients des polluposteurs qui les paient pour diffuser leur publicité. On peut assurément invoquer ces dispositions pour faire échec aux activités des polluposteurs. La législation sur la protection de la vie privée peut aussi être invoquée dans la mesure où ces activités se produisent au Canada.

Dans quelques années on pourrait se rendre compte qu'on a essayé la voie législative, mais qu'elle ne convient pas pour régler les problèmes de ce genre d'activité. Le pourriel est un outil dont on se sert pour se livrer à des activités criminelles interdites par d'autres lois. Peut-être faudra-t-il recourir un jour au projet de loi du sénateur Oliver, mais pour l'instant, il faut se servir de la

obligations for ISPs and legitimate commercial e-mails, you see that we have all the different pieces in place.

Senator Corbin: Senator Oliver told us that there were 15 principal sources of spammers. There may be many more, but of lesser importance. Are those 15 sources known?

Mr. Thomson: For the most part, yes they are known.

Senator Corbin: Why do you not hire them to get rid of them?

Mr. Thomson: I do not think we could afford to do that. They make much more money spamming than we could ever pay them to not spam.

Senator Corbin: You could not buy them out; that is interesting.

I would like to know about the next generation of aggressive and annoying Internet monsters that are beginning to raise their ugly heads and claw at our computers in the name of liberty and freedom of expression. Surely, once you solve the anti-spam problem, the industry will have to face other situations that are evolving only now. You are probably aware of those challenges. Could you take us into your confidence?

Mr. Thomson: It is fair to say that we know of some of the challenges we will have to face in the near future. At the same time, the way in which the Internet is developing, there will be applications, products and services that we just cannot imagine right now.

With respect to the ones that challenge us now, and will challenge us increasingly, viruses are clearly the main problem. That entails dealing with the hijacking of computers for either illegal purposes, through viruses, or just because someone wants to prove that they are able to do it. A phenomenon known as "phishing" is the fraudulent sending of messages by someone disguised as a legitimate source, such as a bank or an Internet service provider or some other organization that collects your personal information so they can do business with you. They indicate that they need some of that information now in order to provide you with further services or to correct a problem within their system, thereby getting you to hand over personal information, credit card information, et cetera, which is then used for criminal purposes. That problem is increasing. It is somewhat associated with the spam problem because much of the phishing activity occurs in bulk and is unsolicited. The police will certainly get involved in that area, which will be of great concern not only to ISPs, but also to end-users.

Ms. Morin: I was going to mention phishing as a problem as well. It has raised the interest of the law enforcement agencies because of the kind of personal information being asked for in that context, such as credit card number, social insurance number

législation existante. Avant d'imposer de nouvelles obligations aux fournisseurs et aux expéditeurs de messages électroniques commerciaux légitimes, on peut comparer les législations des autres pays et on verra que nous avons déjà en main toutes les mesures nécessaires.

Le sénateur Corbin: Le sénateur Oliver nous a dit qu'il y avait 15 grandes sources de polluposteurs. Il peut y en avoir plus, mais elles sont moins importantes. Connaît-on ces 15 sources?

M. Thomson: Oui, dans la plupart des cas.

Le sénateur Corbin: Pourquoi ne les embauchez-vous pas pour vous en débarrasser?

M. Thomson: Je ne pense pas que nous en aurions les moyens. Ils font beaucoup plus d'argent à envoyer des pourriels que nous ne pourrions leur en donner pour ne pas le faire.

Le sénateur Corbin: Donc, vous ne pourriez pas les acheter. Très intéressant.

Je voudrais que vous nous parliez de la prochaine génération de monstres agressifs et insupportables de l'Internet, ceux qui ne font que commencer à assiéger nos ordinateurs au nom de la liberté d'expression. Quand vous aurez réglé le problème du pourriel, l'industrie devra faire face à d'autres situations qui se préparent en ce moment. Vous êtes sans doute au courant de ces défis. Pourriez-vous nous en faire part?

M. Thomson: Nous connaissons certains des défis qui se poseront dans un proche avenir, c'est vrai. Toutefois, d'après la façon dont l'Internet évolue, il y aura des applications, des produits et des services que nous ne pouvons même pas encore imaginer.

Quant aux problèmes qui se posent dès maintenant et qui continueront à se présenter de plus en plus, il s'agit manifestement de virus dans la plupart des cas. Il y a des gens qui s'attaquent aux ordinateurs soit pour des fins illégales, au moyen de virus, soit tout simplement pour prouver qu'ils en sont capables. Nous assistons aussi à un nouveau phénomène, connu sous le nom de «phishing»; il s'agit de l'envoi frauduleux de messages par quelqu'un qui se fait passer pour une source légitime d'information, comme une banque ou un fournisseur de services Internet ou une autre organisation qui recueille de l'information personnelle à votre sujet afin de faire affaire avec vous. L'expéditeur indique qu'il a besoin de certains renseignements pour vous fournir des services ou pour corriger une erreur dans son système, ce qui vous amène à donner de l'information personnelle, votre numéro de carte de crédit par exemple, qui est ensuite utilisée à des fins criminelles. Ce problème prend de plus en plus d'ampleur. Il est associé avec le pourriel parce que beaucoup d'activités de «phishing» se font par des envois massifs non sollicités. La police ne manquera pas de s'attaquer à ce problème qui causera beaucoup d'ennuis non seulement aux fournisseurs de services Internet mais aussi aux utilisateurs de ce service.

Mme Morin: J'allais également mentionner les arnaques de type «phishing». Les corps policiers s'y intéressent à cause de la nature des renseignements personnels qu'on demande, comme le numéro de carte de crédit, le numéro d'assurance sociale et le mot

and bank password. As these new horrors come on board, it emphasizes the fact that awareness and education campaigns must take place, teaching users how to be Web savvy. For example, an ISP might say that you would never receive such an e-mail request for information from them, because if they needed the information, they would ask for it in a different way; so it is necessary to educate your users.

Sympatico was phished last year through a server in the U.S. People automatically asked whom they should be telling. Call the company being replicated and ask if it is really their Web site. We can take steps to change it quickly. There will always be something else, but now that we have these connections amongst ISPs and they talking to each other, rather than doing something drastic, we will call them and ask if they knew about this — do something about this. Other than the phishing, the worms and the viruses, those are the flavour of the day, as it were.

Senator Corbin: Finally, could you give us a sampling of the numbers of people in the ISPs whose work is totally dedicated to fighting these annoyances? Is it 1 per cent overall, or more?

Mr. Thomson: In a small ISP operation, where they have an average of six employees, one person is typically dedicated to dealing with spam.

A larger organization such as ours, TELUS, has 25,000 employees. I cannot tell you the number, because people share responsibilities. However, we certainly have departments that deal with abuse and consumer issues, which obviously include spam problems.

Senator Corbin: Could that be in the hundreds, less or more?

Mr. Thomson: I am hazarding a guess, but it is probably a couple of dozen.

Ms. Morin: They would be involved on the technology side and network operations to keep servers up and running when a new form of spam or virus comes out. Many of them share responsibilities, so they are responsible for technology for the entire service and other different bits and pieces. We have created internal task forces of a dozen people who get together once a week to discuss what they are doing to deal with matters.

All organizations are working to keep spam from coming in to their own employees because of the lost productivity factor in having to weed through 50 or 60 e-mails a day. Organizations must deal with matters from their own business operation side as

de passe permettant d'avoir accès aux comptes en banque. Avec l'avènement de ces nouvelles horreurs, il sera d'autant plus important d'effectuer des campagnes de sensibilisation et d'éducation pour apprendre aux gens à être des internautes avisés. Par exemple, un FSI pourrait dire qu'il n'enverrait jamais de telle demande d'informations par courriel, parce que s'il avait besoin d'informations, il utiliserait un autre moyen; il faut donc éduquer les utilisateurs d'Internet.

L'année dernière, le réseau Sympatico a fait l'objet d'une attaque de «phishing» par l'entremise d'un serveur situé aux États-Unis. Les gens ont demandé qui ils devaient en aviser. Il faut appeler la compagnie dont on a utilisé le nom pour demander s'il s'agit vraiment de son site Web. Dans ce cas, on peut le changer rapidement. Il y aura toujours de nouvelles attaques, mais maintenant les FSI sont reliés entre eux et qu'ils communiquent au lieu de prendre des mesures radicales, on peut les appeler puis leur demander s'ils étaient au courant — afin de réagir. Outre les arnaques du type «phishing», ce sont les vers et les virus informatiques qui posent actuellement le plus de problèmes.

Le sénateur Corbin: Finalement, pourriez-vous nous donner une idée du nombre d'employés des FSI qui ont pour unique tâche de combattre ces problèmes irritants? Est-ce 1 p. 100 ou plus?

M. Thomson: Chez un petit FSI, qui compte en moyenne six employés, une personne est généralement chargée exclusivement de contrer le pourriel.

Une grosse entreprise comme la nôtre, TELUS, compte 25 000 employés. Je ne pourrais vous dire combien d'entre eux sont affectés à cette tâche, parce que les responsabilités sont partagées entre plusieurs employés. Toutefois, nous avons des services qui s'occupent des activités frauduleuses et des services à la clientèle, ce qui comprend évidemment les problèmes de pourriel.

Le sénateur Corbin: Y en a-t-il des centaines? Plus ou moins que cela?

M. Thomson: Je dirais probablement quelques douzaines, mais je ne pourrais pas le dire avec certitude.

Mme Morin: Ils travailleraient du côté des opérations techniques et des opérations de réseau pour maintenir le fonctionnement des serveurs lors d'attaque de nouveaux virus ou de nouveaux genres de pourriel. Beaucoup de ces employés ont d'autres responsabilités également; ils peuvent être chargés du soutien technique pour le service tout entier et d'autres fonctions éparpillées. Nous avons mis sur pied des groupes de travail interne composés d'une douzaine de personnes qui se réunissent une fois par semaine pour discuter de ce qu'ils font pour combattre de tels problèmes.

Toutes les entreprises s'efforcent de prévenir l'envoi de pourriel à leurs employés parce que cela entraîne des pertes de productivité si ceux-ci doivent dépouiller 50 ou 60 courriels chaque jour. Elles doivent s'attaquer aux problèmes sur le plan du fonctionnement

well as their own employees. I cannot tell you exactly how many, but it is increasing.

Senator Corbin: In the end, it adds up to a negative production cost.

Ms. Morin: Absolutely.

Senator Corbin: That cost represents hundreds of thousands of dollars, or more?

Mr. Thomson: It is certainly a case of money going out without any money coming in.

The Chairman: On a point of clarification, TELUS's 25,000 employees are not all involved in providing Internet service?

Mr. Thomson: That is correct.

The Chairman: How many would you have in the ISP portion?

Mr. Thomson: I do not have that number.

Senator Day: Bell Canada and TELUS both went into the Internet business from another business, or added it on to another business. The telephone has been used and continues to be used for unsolicited calls. That does not seem to have become the same kind of problem as on the Internet. Why is that?

Ms. Morin: There are rules about unwanted telemarketing. However, unsolicited faxes are a real thorn in some people's side. There is a cost to the individual sending the fax, but the bulk of the cost is to the individuals at the other end, who are seeing their paper and ink cartridges being used up, and at the same time, are unable to receive legitimate faxes.

While inroads have been made in dealing with those issues, it is still a problem. However, there is not the same volume and there is a real cost for the telemarketers. They would like to be calling only people they think might actually be interested in what they are selling, to cut down their costs. That is why the problem on the telephone side is not as great.

Senator Day: That brings us back to Madam Chairman's questions about market forces controlling this somewhat.

According to the business model for creating an Internet service provider, you must go out and get customers who wish to use ISPs as a portal. Is there any exchange of money? When you sign up to TELUS or Bell Canada's system, once you have an Internet service system set up, is there any exchange of money between you and the other Internet service providers on the Web, or is all your revenue coming from your customer base?

Mr. Thomson: Once a smaller ISP has set up their system, bought their hardware and spent their marketing money to acquire customers, they have ongoing payments to some larger ISPs like Bell or TELUS because they rely on us for network connections to the broader Internet and access to our telecommunications facilities and infrastructure. They can then connect with other ISPs around the world.

de l'entreprise et du côté de leurs propres employés. Je ne pourrais pas vous dire combien sont chargés de cette fonction, mais leur nombre augmente.

Le sénateur Corbin: En définitive, cela occasionne des coûts de production négatifs.

Mme Morin: Absolument.

Le sénateur Corbin: Ce coût peut s'élever à des centaines de milliers de dollars ou plus?

M. Thomson: Ce que je peux vous dire, c'est que cet argent est dépensé en pure perte puisqu'il ne rapporte rien.

La présidente: J'aimerais avoir quelques précisions. Les 25 000 employés de TELUS ne sont pas tous affectés à la fourniture de services Internet, n'est-ce pas?

M. Thomson: C'est exact.

La présidente: Combien y en aurait-il qui s'occupent de la fourniture de services Internet?

M. Thomson: Je n'ai pas ce renseignement.

Le sénateur Day: Bell Canada et TELUS se sont tous les deux orientés vers les services Internet à partir d'autres genres d'activités, ou ont ajouté ce volet à leurs activités. Le téléphone a été utilisé par le passé et il l'est encore pour faire des appels non sollicités. Dans ce cas, cela ne semble pas avoir causé un problème aussi grave que ce que l'on voit sur Internet. Pourquoi?

Mme Morin: Il y a des règles qui s'appliquent au télémarketing. Cependant, les fax non sollicités sont un véritable fléau pour certains. L'expéditeur du fax paye un certain coût, mais l'essentiel du coût est supporté par les destinataires, qui doivent payer le papier et l'encre, et qui pendant ce temps, ne peuvent pas recevoir des fax légitimes.

Même si on a fait des progrès pour combattre ces problèmes, ils existent toujours. Le volume n'est cependant pas le même et ceux qui font du télémarketing assument des coûts réels. Ils voudraient bien n'appeler que les gens qui pourraient être intéressés par leurs produits, afin de réduire leurs coûts. Voilà pourquoi le problème n'atteint pas les mêmes proportions.

Le sénateur Day: Cela me ramène aux questions de madame la présidente au sujet des forces du marché.

D'après le modèle de gestion qu'il faut suivre pour mettre sur pied une entreprise fournissant des services Internet, vous devez aller chercher des clients désireux d'utiliser un portail de FSI. Y a-t-il échange d'argent? Quand on s'abonne au système de TELUS ou de Bell Canada, une fois que le système est fonctionnel, y a-t-il échange d'argent entre vous et d'autres fournisseurs Internet sur le Web, ou est-ce que tous vos revenus proviennent de vos clients?

M. Thomson: Quand un petit FSI a mis sur pied son système, acheter le matériel et fait le marketing nécessaire pour trouver des clients, il doit payer régulièrement un certain montant à un gros FSI comme Bell ou TELUS parce qu'il a besoin de connexions de réseau à Internet a aussi il doit avoir accès à nos installations de télécommunications et à notre infrastructure. Cela lui permet de se relier à d'autres FSI dans le monde.

Companies of our size have revenue coming in from end-users and from other ISPs. Smaller companies have revenue coming in from their customers and expenses going out to everyone else.

Senator Day: As a large Internet service provider, do you pay to connect to the World Wide Web? Do you have money going out in that regard?

Mr. Thomson: We have expenses as well. We must enter into relationships with other providers.

Ms. Morin: Those providers will carry our e-mail traffic, just as we will carry theirs.

Senator Day: Would that not provide for some financial incentive? Would that not control the volume? Is that the reason that you would want to ensure that you do not send material along the line that you do not want on there? Would that not be the same coming the other way? Is there not a market force in there that would help achieve some control?

Mr. Thomson: There is a huge financial incentive to try to control this. However, we do not have the financial tools to do so. We need these other pieces of the pie, parts of the menu, to help us.

Senator Day: Have you told us about all of the other financial tools that you need? Have we talked about that today? Is there something more you wish to tell us?

Ms. Morin: I think Mr. Thomson was alluding to the other pieces of the multi-faceted approach that we have talked about already.

Senator Day: I just wish to ensure that we know who is dealing with you in relation to Industry Canada. We talked earlier about their action plan. You have participated with Industry Canada in the action plan; is that correct?

Mr. Thomson: Yes.

Senator Day: You talk back and forth.

Mr. Thomson: We have consulted frequently.

Senator Day: Can you tell us a few names of people so that we could bring them here to tell us where they are? You may wish to send us those contact names to ensure that we go to the right people.

Ms. Morin: We have been dealing with Michael Binder and the individuals who work with him.

The Chairman: We already have that information.

Ms. Morin and Mr. Thomson, thank you for an interesting session. We are learning. We are very grateful to you for taking the time to be with us. It was obviously very important for us to hear from you, and rest assured, it matters.

The committee adjourned.

Les grosses entreprises comme la nôtre tirent leur revenu des utilisateurs individuels et des autres FSI. Les petites compagnies tirent leur revenu de leurs clients et doivent dépenser de l'argent à d'autres égards.

Le sénateur Day: Étant un gros fournisseur de services Internet, devez-vous payer pour vous connecter au Web? Est-ce que cela fait partie de vos dépenses?

M. Thomson: Nous avons également des dépenses. Nous devons conclure des ententes avec d'autres fournisseurs.

Mme Morin: Ces fournisseurs acheminent nos courriels, tout comme nous acheminons les leurs.

Le sénateur Day: Est-ce que ce ne serait pas là une incitation financière? Est-ce que cela ne contribuerait pas à contenir le volume? Pour cette raison, ne voudriez-vous pas vous assurer de ne pas acheminer de courriels indésirables? Et les autres fournisseurs ne feraient-ils pas de même? N'y a-t-il pas là une force du marché qui pourrait contribuer à assurer un certain contrôle?

M. Thomson: Il y a effectivement une incitation financière colossale à contenir ces courriels. Cependant, nous n'avons pas les outils financiers pour le faire. Il faudrait que nous ayons d'autres morceaux du casse-tête, d'autres parties du menu.

Le sénateur Day: Nous avez-vous parlé de tous les autres outils financiers dont vous avez besoin? Ont-ils été abordés aujourd'hui? Y a-t-il autre chose que vous souhaitez nous communiquer?

Mme Morin: Je pense que M. Thomson faisait allusion aux autres éléments de l'approche sur plusieurs fronts que nous avons déjà expliquée.

Le sénateur Day: Je veux que nous sachions qui s'occupe de vous à Industrie Canada. Nous avons évoqué leur plan d'action tout à l'heure. Vous avez participé à l'élaboration de ce plan d'action avec Industrie Canada, n'est-ce pas?

M. Thomson: Oui.

Le sénateur Day: Il y a une communication dans les deux sens.

M. Thomson: Nous avons souvent été consultés.

Le sénateur Day: Pourriez-vous nous donner le nom des fonctionnaires avec lesquels vous avez fait affaire pour que nous puissions les inviter à venir faire le point sur ce dossier devant notre comité? Il sera peut-être bon de nous envoyer le nom de vos contacts pour que nous nous adressions aux bonnes personnes.

Mme Morin: Nous traitons avec Michael Binder et les gens de son équipe.

La présidente: Nous avons déjà cette information.

Madame Morin et monsieur Thomson, je vous remercie pour cette séance fort intéressante. Nous avons appris beaucoup de choses. Nous vous sommes reconnaissants d'avoir bien voulu assister à notre réunion. Il est naturellement très important pour nous d'entendre votre point de vue et je vous assure que nous en tiendrons compte.

La séance est levée.

WITNESSES

From the Canadian Association of Internet Providers:

Jay Thomson, Former President;

Suzanne Morin, Member of the Spam Committee.

TÉMOINS

De l'Association canadienne des fournisseurs Internet:

Jay Thomson, ancien président;

Suzanne Morin, membre du comité sur le pourriel.

Available from:
PWGSC – Publishing and Depository Services
Ottawa, Ontario K1A 0S5
Also available on the Internet: http://www.parl.gc.ca

Disponible auprès des:
TPGSC – Les Éditions et Services de dépôt
Ottawa (Ontario) K1A 0S5
Aussi disponible sur internet: http://www.parl.gc.ca