Second Session
Fortieth Parliament, 2009

SENATE OF CANADA

Proceedings of the Standing Senate Committee on

Legal and Constitutional Affairs

Chair:
The Honourable JOAN FRASER

Wednesday, May 13, 2009
Thursday, May 14, 2009

Issue No. 8

First and second meetings on:

Bill S-4, An Act to amend the Criminal Code (identity theft and related misconduct)

APPEARING:
The Honourable Rob Nicholson, P.C., M.P.,
Minister of Justice and Attorney General of Canada

WITNESSES:
(*See back cover*)

Deuxième session de la
quarantième législature, 2009

SÉNAT DU CANADA

Délibérations du Comité sénatorial permanent des

Affaires juridiques et constitutionnelles

Présidente :
L'honorable JOAN FRASER

Le mercredi 13 mai 2009
Le jeudi 14 mai 2009

Fascicule nº 8

Première et deuxième réunions concernant :

Le projet de loi S-4, Loi modifiant le Code criminel (vol d'identité et inconduites connexes)

COMPARAÎT :
L'honorable Rob Nicholson, C.P., député,
ministre de la Justice et procureur général du Canada

TÉMOINS :
(*Voir à l'endos*)

47224-47228

THE STANDING SENATE COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS

The Honourable Joan Fraser, *Chair*

The Honourable Pierre Claude Nolin, *Deputy Chair*

and

The Honourable Senators:

Angus	Joyal, P.C.
Baker, P.C.	* LeBreton, P.C.
Bryden	(or Comeau)
Campbell	Milne
* Cowan	Rivest
(or Tardif)	Wallace
Dickson	Watt

*Ex officio members

(Quorum 4)

Changes in membership of the committee:

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

The Honourable Senator Watt replaced the Honourable Senator Merchant (*May 14, 2009*).

The Honourable Senator Dickson replaced the Honourable Senator Stratton (*May 14, 2009*).

The Honourable Senator Merchant replaced the Honourable Senator Watt (*May 13, 2009*).

The Honourable Senator Stratton replaced the Honourable Senator Dickson (*May 13, 2009*).

The Honourable Senator Bryden replaced the Honourable Senator Rompkey, P.C. (*May 7, 2009*).

LE COMITÉ SÉNATORIAL PERMANENT DES AFFAIRES JURIDIQUES ET CONSTITUTIONNELLES

Présidente : L'honorable Joan Fraser

Vice-président : L'honorable Pierre Claude Nolin

et

Les honorables sénateurs :

Angus	Joyal, C.P.
Baker, C.P.	* LeBreton, C.P.
Bryden	(ou Comeau)
Campbell	Milne
* Cowan	Rivest
(ou Tardif)	Wallace
Dickson	Watt

* Membres d'office

(Quorum 4)

Modifications de la composition du comité :

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

L'honorable sénateur Watt a remplacé l'honorable sénateur Merchant (*le 14 mai 2009*).

L'honorable sénateur Dickson a remplacé l'honorable sénateur Stratton (*le 14 mai 2009*).

L'honorable sénateur Merchant a remplacé l'honorable sénateur Watt (*le 13 mai 2009*).

L'honorable sénateur Stratton a remplacé l'honorable sénateur Dickson (*le 13 mai 2009*).

L'honorable sénateur Bryden a remplacé l'honorable sénateur Rompkey, C.P. (*le 7 mai 2009*).

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

ORDER OF REFERENCE

Extract from the *Journals of the Senate*, Tuesday, May 5, 2009:

Resuming debate on the motion of the Honourable Senator Wallace, seconded by the Honourable Senator St. Germain, P.C., for the second reading of Bill S-4, An Act to amend the Criminal Code (identity theft and related misconduct).

After debate,

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

The bill was then read the second time.

The Honourable Senator Wallace moved, seconded by the Honourable Senator Nolin, that the bill be referred to the Standing Senate Committee on Legal and Constitutional Affairs.

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

ORDRE DE RENVOI

Extrait des *Journaux du Sénat* du mardi 5 mai 2009 :

Reprise du débat sur la motion de l'honorable sénateur Wallace, appuyée par l'honorable sénateur St. Germain, C.P., tendant à la deuxième lecture du projet de loi S-4, Loi modifiant le Code criminel (vol d'identité et inconduites connexes).

Après débat,

La motion, mise aux voix, est adoptée.

Le projet de loi est alors lu pour la deuxième fois.

L'honorable sénateur Wallace propose, appuyé par l'honorable sénateur Nolin, que le projet de loi soit renvoyé au Comité sénatorial permanent des affaires juridiques et constitutionnelles.

La motion, mise aux voix, est adoptée.

Le greffier du Sénat,

Paul C. Bélisle

Clerk of the Senate

MINUTES OF PROCEEDINGS

OTTAWA, Wednesday, May 13, 2009
(15)

[*English*]

The Standing Senate Committee on Legal and Constitutional Affairs met this day at 4:01 p.m., in room 257, East Block, the chair, the Honourable Joan Fraser, presiding.

Members of the committee present: The Honourable Senators Angus, Baker, P.C., Bryden, Fraser, Joyal, P.C., Merchant, Milne, Nolin, Stratton and Wallace (10).

In attendance: Dominique Valiquet and Carolina Mingarelli, Analysts, Parliamentary Information and Research Service, Library of Parliament.

Also in attendance: The official reporters of the Senate.

Pursuant to the order of reference adopted by the Senate on Tuesday, May 5, 2009, the committee began its consideration of Bill S-4, An Act to amend the Criminal Code (identity theft and related misconduct).

APPEARING:

The Honourable Rob Nicholson, P.C., M.P., Minister of Justice and Attorney General of Canada.

WITNESS:

Department of Justice Canada:

Joanne Klineberg, Counsel, Criminal Law Policy Section.

The chair made an opening statement.

Mr. Nicholson, P.C., M.P., made a statement and, together with Ms. Klineberg, answered questions.

At 5:18 p.m., the committee suspended.

At 5:19 p.m., the committee resumed.

Ms. Klineberg continued answering questions.

At 5:59 p.m., the committee adjourned to the call of the chair.

ATTEST:

OTTAWA, Thursday, May 14, 2009
(16)

[*English*]

The Standing Senate Committee on Legal and Constitutional Affairs met this day at 10:47 a.m., in room 257, East Block, the chair, the Honourable Joan Fraser, presiding.

Members of the committee present: The Honourable Senators Baker, P.C., Bryden, Campbell, Dickson, Fraser, Joyal, P.C., Milne, Nolin and Wallace (9).

PROCÈS-VERBAUX

OTTAWA, le mercredi 13 mai 2009
(15)

[*Traduction*]

Le Comité sénatorial permanent des affaires juridiques et constitutionnelles se réunit aujourd'hui, à 16 h 1, dans la salle 257 de l'édifice de l'Est, sous la présidence de l'honorable Joan Fraser, (*présidente*).

Membres du Comité présents : Les honorables sénateurs Angus, Baker, C.P., Bryden, Fraser, Joyal, C.P., Merchant, Milne, Nolin, Stratton et Wallace (10).

Également présents : Dominique Valiquet et Carolina Mingarelli, analystes, Service d'information et de recherche parlementaires, Bibliothèque du Parlement.

Aussi présents : Les sténographes officiels du Sénat.

Conformément à l'ordre de renvoi adopté par le Sénat le mardi 5 mai 2009, le comité entreprend son examen du projet de loi S-4, Loi modifiant le Code criminel (vol d'identité et inconduites connexes).

COMPARAÎT :

L'honorable Rob Nicholson, C.P., député, ministre de la Justice et procureur général du Canada.

TÉMOIN :

Ministère de la Justice Canada :

Joanne Klineberg, avocate, Section de la politique en matière de droit pénal.

La présidente fait une déclaration.

M. Nicholson, C.P., député, fait un exposé, puis avec l'aide de Mme Klineberg, répond aux questions.

À 17 h 18, le comité suspend ses travaux.

À 17 h 19, le comité reprend ses travaux.

Mme Klineberg continue de répondre aux questions.

À 17 h 59, le comité suspend ses travaux jusqu'à nouvelle convocation de la présidence.

ATTESTÉ :

OTTAWA, le jeudi 14 mai 2009
(16)

[*Traduction*]

Le Comité sénatorial permanent des affaires juridiques et constitutionnelles se réunit aujourd'hui, à 10 h 47, dans la salle 257 de l'édifice de l'Est, sous la présidence de l'honorable Joan Fraser (*présidente*).

Membres du comité présents : Les honorables sénateurs Baker, C.P., Bryden, Campbell, Dickson, Fraser, Joyal, C.P., Milne, Nolin et Wallace (9).

In attendance: Dominique Valiquet and Carolina Mingarelli, Analysts, Parliamentary Information and Research Service, Library of Parliament.

Also in attendance: The official reporters of the Senate.

Pursuant to the order of reference adopted by the Senate on Tuesday, May 5, 2009, the committee continued its consideration of Bill S-4, An Act to amend the Criminal Code (identity theft and related misconduct).

WITNESSES:

Information Technology Association of Canada:

David McMahon, Advisor, National Security — Bell Canada.

Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic:

David Fewer, Acting Director;

Tamir Israel, Articling student.

The chair made an opening statement.

Mr. McMahon made a statement and answered questions.

At 11:59 a.m., the committee suspended.

At 12:01 p.m., the committee resumed.

Mr. Fewer made a statement and, together with Mr. Israel, answered questions.

At 12:49 p.m., the committee adjourned to the call of the chair.

ATTEST:

Également présents : Dominique Valiquet et Carolina Mingarelli, analystes, Service d'information et de recherche parlementaires, Bibliothèque du Parlement.

Aussi présents : Les sténographes officiels du Sénat.

Conformément à l'ordre de renvoi adopté par le Sénat le mardi 5 mai 2009, le comité poursuit son examen du projet de loi S-4, Loi modifiant le Code criminel (vol d'identité et inconduites connexes).

TÉMOINS :

Association canadienne de la technologie de l'information :

David McMahon, conseiller, Sécurité nationale — Bell Canada.

Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko :

David Fewer, directeur intérimaire;

Tamir Israel, stagiaire au droit.

La présidente fait une déclaration.

M. McMahon fait un exposé puis répond aux questions.

À 11 h 59, le comité suspend ses travaux.

À 12 h 1, le comité reprend ses travaux.

M. Fewer fait un exposé puis, avec l'aide de M. Israel, répond aux questions.

À 12 h 49, le comité suspend ses travaux jusqu'à nouvelle convocation de la présidence.

ATTESTÉ :

La greffière du comité,

Jessica Richardson

Clerk of the Committee

EVIDENCE

OTTAWA, Wednesday, May 13, 2009

The Standing Senate Committee on Legal and Constitutional Affairs met this day at 4:01 p.m. to study Bill S-4, An Act to amend the Criminal Code (identity theft and related misconduct).

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

[*Translation*]

The Chair: Welcome to this meeting of the Standing Senate Committee on Legal and Constitutional Affairs. We will begin our study of Bill S-4, An Act to amend the Criminal Code (identity theft and related misconduct).

[*English*]

This is an extremely interesting bill. We have the pleasure of having with us as our first witness on this bill the sponsoring minister, the Honourable Rob Nicholson, P.C., M.P., Minister of Justice and Attorney General of Canada. He is familiar with this committee and has had cause to appear before us a number of times because that is the nature of being the Minister of Justice: You get to appear often before the Legal Committee.

We are glad to welcome you, minister. We await with interest your opening statement and then will ask you questions. The floor is yours.

The Hon. Rob Nicholson, P.C., M.P., Minister of Justice and Attorney General of Canada: Thank you very much, Madam Chair. I am always pleased to appear on behalf of another piece of justice legislation. I welcome the new members of the committee and thank Senator Wallace for introducing this bill at the Senate level. It is much appreciated and is something that will be welcomed across this country.

The amendments contained in Bill S-4 address the growing concerns about identity-related crimes in this country. The criminal misuse of identity is not a new problem, but it has taken on a new life and new dimensions. This is what law enforcement agencies and across this country have been telling me.

[*Translation*]

Criminals have always hidden their true identities and used fake ones. What has changed in recent decades is that we are putting more and more trust in technology.

[*English*]

We enjoy much greater security and protection, but criminals also enjoy new opportunities to obtain greater illicit benefits at less risk. The government believes these new threats can and must be addressed in the Criminal Code.

TÉMOIGNAGES

OTTAWA, le mercredi 13 mai 2009

Le Comité permanent des affaires juridiques et constitutionnelles se réunit aujourd'hui, à 16 1 heures, pour étudier le projet de loi S-4, Loi modifiant le Code criminel (vol d'identité et inconduites connexes).

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

[*Français*]

La présidente : Bienvenue au Comité des affaires juridiques et constitutionnelles. Nous entamons notre étude du projet de loi S-4, Loi modifiant le Code criminel (vol d'identité et inconduites connexes).

[*Traduction*]

C'est un projet de loi extrêmement intéressant. Nous avons le plaisir d'avoir avec nous notre premier témoin qui est le ministre qui parraine ce projet, l'honorable Rob Nicholson, C.P., député, ministre de la Justice et procureur général du Canada. Il connaît bien ce comité, il a eu de nombreuses fois l'occasion d'y témoigner puisque la nature de son poste, ministre de la Justice, commande de témoigner souvent devant le comité juridique.

Nous sommes heureux de vous avoir avec nous, monsieur le ministre et nous attendons avec intérêt votre déclaration d'ouverture, ensuite nous vous poserons des questions. La parole est à vous.

L'honorable Rob Nicholson, C.P., député, ministre de la Justice et procureur général du Canada : Merci beaucoup, madame la présidente. Je suis toujours heureux de venir défendre un nouveau projet de loi. Je souhaite la bienvenue aux nouveaux membres de ce comité et remercie le sénateur Wallace pour avoir introduit ce projet de loi au Sénat. Ce projet est très apprécié et sera bien accueilli dans tout le pays.

Les modifications contenues dans le projet de loi S-4 s'attaquent à des préoccupations grandissantes concernant les crimes liés à l'identité commis au pays. L'utilisation de l'identité à des fins criminelles n'est pas un problème nouveau, mais il a pris de nouvelles dimensions. C'est ce que les organismes d'application de la loi d'un bout à l'autre du pays me disent.

[*Français*]

Les criminels ont toujours dissimulé leur vraie identité et en ont emprunté des fausses. Ce qui a changé au cours des dernières décennies est le fait que nous faisons de plus en plus confiance à la technologie.

[*Traduction*]

Nous jouissons d'une plus grande protection, mais les criminels eux jouissent de nouvelles occasions pour obtenir de meilleurs avantages illicites à moindres risques. Le gouvernement estime que le Code criminel peut et doit se pencher sur ces nouvelles menaces.

In Canada, we have always had some identity-based offences. This includes most directly the offence of personation and also secondary offences such as forgery of documents — including identity documents — fraud, misuse of credit cards and offences to protect specific forms of identification, such as the Canadian passport.

This bill makes some changes to modernize these long-standing offences. However, its main purpose is the creation of new offences that focus specifically on the early stages of abuses of identification and identity information.

These new offences can be applied before offenders have a chance to misuse personal information. We believe this is important for several reasons. First, it recognizes that, in the modern era, identity crime generates distinct groups of victims. The economic harm to victims of secondary offences, such as fraud and credit card misuse, has always been addressed by the Criminal Code. However, people's reputations, credit-worthiness and even criminal liability may be affected. These victims suffer harm whether other crimes are committed with identity information or not and the damage is very difficult to correct.

Second, the proposed new measures will close gaps created by new technologies and new crimes. Taking physical documents may be theft under existing law, but simply copying information is not addressed by traditional property offences. In this context, criminal groups have learned to specialize and cooperate with one another. One may steal or fabricate information, another may produce physical or electronic documents for sale, and the end users of the identities then commit other crimes with them.

Third, from a more practical standpoint, the new offences enable law enforcement agencies to become engaged at earlier stages of the criminal schemes. This could result in a reduction of more serious types of victimization.

Fourth, identity-related crime is a rapidly expanding problem at the international level. The government has been engaged in raising this issue in international fora for some time. I raised it myself with the G8 justice ministers in Tokyo last year, and I will be raising it again with my colleagues this year to make them aware of the implications and the challenges we all face.

By bring forward these amendments, Canada will be sending a strong message to other countries that we take the problem seriously and are committed to doing something about it.

I propose to leave some of the more technical amendments for your questions, but I will now turn to what I believe are the key amendments in the package. The first element of the bill would form a new section 56.1 to the Criminal Code and criminalize the

Au Canada, nous avons toujours eu des infractions liées à l'identité. En particulier l'usurpation d'identité et d'autres infractions secondaires comme la falsification de documents — notamment les pièces d'identité — la fraude, l'utilisation criminelle des cartes de crédit et des infractions qui touchent la protection de pièces d'identité précises comme le passeport canadien.

Ce projet de loi propose quelques changements qui moderniseront ces infractions qui existent depuis longtemps. Cependant, son objectif principal est la création de nouvelles infractions qui visent précisément les étapes préparatoires au vol et à l'utilisation abusive de renseignements d'identité.

Ces nouvelles infractions peuvent être appliquées avant que les délinquants aient la chance d'utiliser les renseignements personnels. Nous croyons que cela est important pour plusieurs raisons. Premièrement, il s'agit de reconnaître en cette ère moderne que les crimes contre l'identité créent un groupe de victimes distinct. Les dommages économiques que les victimes d'infractions secondaires, telles que la fraude et l'utilisation criminelle de cartes de crédit, ont toujours été ciblés dans le Code criminel. Cependant, la réputation des gens, les cotes de crédit et même la responsabilité criminelle peuvent être affectées. Ces victimes subissent des dommages sans égard au fait que des crimes soient commis avec les renseignements liés à l'identité ou non et ces dommages sont très difficiles à corriger.

Deuxièmement, les nouvelles mesures proposées vont également remplir le fossé créé par les nouvelles technologies et les nouveaux crimes. S'approprier des documents peut être considéré comme un vol selon les lois existantes, mais la copie de ces renseignements n'est pas condamnée comme un crime contre les biens. Dans ce contexte, les groupes criminalisés ont appris à se spécialiser et à coopérer les uns avec les autres. Un groupe peut voler ou fabriquer des renseignements, un autre produira les documents papier ou électroniques et à la fin, des utilisateurs de ces nouvelles identités commettront des crimes.

Troisièmement, d'un point de vue pratique, les nouvelles infractions vont permettre aux organismes d'application de la loi d'intervenir plus tôt dans les étapes d'un schéma criminel. Ceci pourrait avoir comme résultat de réduire les victimes de crimes plus graves.

Quatrièmement, les crimes reliés à l'identité représentent un problème qui évolue rapidement sur le plan international. Le gouvernement s'est engagé à soulever cette question dans les forums internationaux depuis un certain temps. J'ai moi-même soulevé la question avec les ministres de la Justice du G8 à Tokyo l'année dernière, et je soulèverai cette question à nouveau avec mes collègues cette année pour les sensibiliser aux défis et aux engagements auxquels nous devons tous faire face.

En apportant ces modifications, le Canada enverra un message fort à tous les autres pays qui dira que nous prenons ce problème très au sérieux et que nous voulons le régler.

Je propose de laisser de côté les modifications plus techniques pour la période de questions, et maintenant j'aimerais vous parler de ce que je crois être les modifications principales dans ce dossier. En premier lieu, le projet de loi propose un nouvel article 56.1 au

procurement, possession, transfer, and sale or offering for sale, of specific physical identity documents. At present, simply possessing or trafficking in other people's identity information is not a crime, and we believe that it should be, of course, subject to the appropriate exceptions.

We have provided those exceptions in proposed new subsection 56.1(2) and, as an added safeguard, the offence also allows for other lawful excuses of a more general nature. For example, a person caught trying to enter Canada with a collection of different passports would probably trigger an investigation, but obviously a parent in possession of a child's passport would have a lawful excuse.

The second key amendment, and the most important change in the package, is composed of four elements: The establishment of a new definition of "identity information"; a new offence of identity theft; a new offence of trafficking in identity information; and the modernization and expansion of the old offence of personation, resulting in a renamed offence of identity fraud.

The proposed new identity theft offence deals primarily with obtaining or possessing identity information in circumstances that show intent to commit one of a series of other related offences. A related offence will be established to cover trafficking in information and knowing or being reckless as to whether it will be used for one of those same offences. Both offences will be guided by a broad definition of identity information, which covers all the types of information that can be used to identify a person.

It is important to note here that, based on the definition, these offences are directed at the mishandling of information. It will not matter whether that information is contained in an official identification document or whether it is merely copied or stored in some other form.

The bill also modifies the offence of personation, the actual impersonating of another person by renaming it "identity fraud." It also clarifies that misuse of a real person's identity for the purpose of evading criminal liability is captured in addition to other improper purposes.

Bill S-4 also allows for an order that the convicted offender pay restitution of the costs of repairing or restoring identity for these offences; and why not? We should be helping out these victims who have been victimized by these individuals. We believe that creating an offence of identity theft, which targets the collection and possession of identity information, coupled with the existing offence of identity fraud presents a more coherent picture of the various stages of identity crime.

Code criminel qui criminalise l'appropriation, la possession, le transfert ainsi que la vente ou l'offre de vente de certains documents d'identité en format papier. En ce moment, la simple possession ou le trafic de renseignements identificateurs d'une autre personne n'est pas un crime et nous pensons que cela devrait l'être, bien sûr avec certaines exceptions justifiées.

Nous avons inscrit ces exceptions dans le nouveau paragraphe 56.1(2) proposé et, à titre de protection supplémentaire, l'infraction prévoit d'autres excuses légitimes de nature plus générale. Par exemple, une personne qui sera surprise à tenter d'entrer au Canada avec une série de différents passeports déclenchera une enquête, mais évidemment, un parent qui est en possession du passeport d'un enfant aura une excuse légitime.

La deuxième modification, et le changement le plus important du dossier, est composée de quatre éléments : l'établissement d'une nouvelle définition de « renseignements identificateurs », une nouvelle infraction de vol d'identité, une nouvelle infraction de trafic de renseignements identificateurs ainsi que la modernisation et l'expansion de l'infraction déjà existante d'usurpation d'identité qui donne lieu à l'infraction nouvellement nommée fraude d'identité.

La nouvelle infraction de vol d'identité proposée s'attaque surtout à l'obtention ou à la possession de renseignements identificateurs dans des circonstances qui montrent une intention de commettre une série d'infractions connexes. Une infraction connexe sera prescrite qui incriminera les personnes qui trafiquent des renseignements et qui savent que ces renseignements pourraient être utilisés à des fins criminelles ou qui ne s'en soucient pas. Chacune de ces infractions sera encadrée par une définition globale des renseignements identificateurs qui couvrent tout type de renseignements qui peuvent servir à identifier une personne.

Il est important de noter que, d'après cette définition, ces infractions visent la mauvaise utilisation de renseignements. Il ne s'agira pas de déterminer si les renseignements sont contenus dans un document officiel d'identification ou s'ils ont été simplement copiés ou stockés sous une autre forme.

Le projet de loi modifie également l'infraction d'usurpation d'identité, le fait de se faire passer pour une autre personne, en lui donnant le nouveau terme de « fraude d'identité ». Il clarifie aussi la mauvaise utilisation de l'identité d'une personne réelle dans le but d'échapper à une responsabilité criminelle en plus d'autres faits répréhensibles.

Le projet de loi S-4 établit également la règle qui force une personne condamnée à réparer les dommages causés par ses infractions. Pourquoi ne pourrions-nous pas aider les victimes qui ont subi des torts aux mains de ces individus? Nous croyons qu'en créant une infraction de vol d'identité, qui cible l'appropriation et la possession de renseignements identificateurs, jumelée avec l'infraction déjà existante de fraude d'identité, nous aurons une image beaucoup plus cohérente des différentes étapes qui composent le crime d'identité.

Bill S-4 also clarifies and extends certain existing offences in the Criminal Code. The bill will improve the law in relation to credit and debit card offences, misconduct in relation to the mail and the forgery regime.

Finally, in proposing these amendments, the government realizes that officials from legitimate investigative agencies often must conceal their identities or impersonate others in the course of undercover investigations. To ensure that law enforcement can work to keep Canadians safe from crime, the bill excludes law enforcement from offences in relation to forged documents for otherwise lawful conduct undertaken in the course of their duties or employment. Agencies that produce identity documents are also exempt if, in good faith and at the request of a government agency, they make false identity documents for use in covert operations.

Madam Chair, this concludes my summary of what I believe to be the key elements of the package for this important piece of legislation. I will do something now that I perhaps should have done at the beginning and introduce Joanne Klineberg from the Department of Justice, who is an expert on the elements of this bill. I am very pleased that she is joining me today.

The Chair: I was the one who should have introduced her, and you took the words out of my mouth. I apologize, Ms. Klineberg. We are very glad to have you with us.

Senator Wallace: Minister Nicholson and Ms. Klineberg, I welcome you here today and thank you for the presentation.

I would like to begin, since I am the sponsor of this bill in the Senate, by saying how proud I was to stand with you, minister, and a number of stakeholders when you announced the tabling of Bill S-4. Those stakeholders, as you will recall, included representatives from Visa, MasterCard, American Express, Interac Association, Equifax and the Canadian Bankers Association, who all applauded you for bringing forward this much anticipated and necessary legislation.

I would like to take a moment to quote from the press release that was issued by the Canadian Bankers Association, which quotes their president, Nancy Hughes Anthony:

> "Currently Canada is the only developed country without legislation designating identity theft as a crime," said Ms. Hughes Anthony. "With this legislation, Canada is poised to move from the back of the pack to the front, because we will have some of the most comprehensive legislation against identity theft in the industrialized world."
>
> Identity theft, the theft of personal information, is currently not illegal but it can lead to a wide variety of crimes — from financial fraud and forgery to real estate fraud and the abuse of government programs.

Le projet de loi S-4 clarifie également et élargit certaines infractions déjà prévues dans le Code criminel. Ce projet de loi va améliorer la loi en ce qui a trait aux infractions liées aux cartes de crédit et de débit, ainsi qu'à l'inconduite relative au courrier et à la contrefaçon.

Finalement, en proposant ces modifications, le gouvernement admet que les agents qui travaillent pour des organismes d'enquête légitimes doivent souvent cacher leur identité ou se faire passer pour une autre personne dans le cadre de leurs enquêtes d'infiltration. Pour faire en sorte que l'application de la loi continue de protéger les Canadiens contre le crime, le projet de loi exclut les infractions liées à la contrefaçon de documents qui sont commises dans le cadre de leur travail ou de leur emploi. Les organismes qui produisent des documents d'identité sont également exemptés si, de bonne foi et à la demande d'un organisme gouvernemental, ils produisent de faux documents d'identité qui seront utilisés au cours d'opérations d'infiltration.

Madame la présidente, ceci met un terme à mon résumé de ce que je crois être les éléments clés du dossier de ce projet de loi important. Je vais faire maintenant quelque chose que j'aurais probablement dû faire dès le début et présenter Johanne Klineberg, du ministère de la Justice, qui est une spécialiste des éléments du projet de loi. Je suis très heureux qu'elle se joigne à nous aujourd'hui.

La présidente : C'est moi qui aurais dû la présenter, et vous m'avez enlevé les mots de la bouche. Je vous demande pardon, madame Klineberg. Nous sommes très heureux de vous avoir avec nous.

Le sénateur Wallace : Monsieur le ministre Nicholson et Mme Klineberg, je vous souhaite la bienvenue aujourd'hui et je vous remercie pour l'exposé.

J'aimerais commencer en disant, puisque je suis le parrain de ce projet de loi au Sénat, que j'étais très fier d'être là avec vous, monsieur le ministre, ainsi que de nombreuses parties intéressées, lorsque vous avez annoncé le dépôt du projet de loi S-4. Parmi les parties intéressées, comme vous vous en souviendrez, il y avait des représentants de Visa, de MasterCard, d'American Express, de l'Association Interac, d'Équifax ainsi que de l'Association des banquiers du Canada qui vous ont tous applaudis pour avoir mis de l'avant ce projet de loi nécessaire et attendu.

J'aimerais citer le communiqué de presse qui a été émis par l'Association des banquiers du Canada et qui cite la présidente Nancy Hughes Anthony :

> « À l'heure actuelle, le Canada est le seul pays développé qui n'a pas de loi définissant le vol d'identité comme étant un crime, affirme Mme Hughes Anthony. Ces mesures législatives permettront au Canada de passer en tête du peloton, parce qu'il se dotera d'une loi contre le vol d'identité parmi les plus élaborées du monde industrialisé. »
>
> Le vol d'identité, le vol de renseignements personnels, n'est actuellement pas illégal, mais peut entraîner un large éventail de crimes, qu'il s'agisse de fraude financière, de falsification, de fraude immobilière et d'abus des programmes gouvernementaux.

"It is important that law enforcement agencies have the tools necessary to stop criminal activity at its earliest root source," said Ms. Hughes Anthony. "There is an urgent need to make identity theft a defined offence — an actual crime — in Canada and we urge all parties to join together and pass this legislation quickly."

Ms. Hughes concluded by stating:

"Minister Nicholson's legislation represents concrete action in the fight against identity theft and we applaud and support his efforts to protect Canadians."

Minister, I know this legislation has been well received by the stakeholders, which is obvious. Is it your sense that this legislation has been well received by Canadians in general?

Mr. Nicholson: It did get pretty good feedback, Senator Wallace. Again, thank you for introducing this bill in the Senate. Canadians know that this is a growing problem. I myself was a victim of identity theft to the extent that my credit card information was transferred to someone in Calgary. It was of interest to me, but the woman who called to inform me did not know who I was or any connection I had. When she called my home to talk to me about this, she said, "I should let you know this is a growing problem in Canada." I said, "You have no idea how interested I am in this subject quite apart from the fact that you are calling me on this."

I have been to Montreal a few times where I sat with people from law enforcement agencies, and they have indicated to me things that I have heard in other communities as well, which is that this is becoming more sophisticated and that the laws have to catch up with what is happening. Our criminal laws were written at a time when the thought was that all crimes were confined here to Canada and this is what happens. Well, these crimes are not confined to Canada any more. Many times this information gets shifted in a split second outside of the country. In fact, the production of the illegal credit cards or the other misuse of people's personal identification many times is not done in Canada. We have this gap in the law where these people who are collecting all this information are not being prosecuted because of gaps in the law.

This is a challenge we always have, frankly, with the Criminal Code of this country. It is not just a question of getting tough on crime. Most of us want to do that, or believe that is important. A bill such as this is basically filling the gaps on the existing Criminal Code legislation. It is something we have to do, and I think it is important. I have had nothing but positive feedback on this bill. I cannot say that for all the legislation. I get pretty good feedback on all of it, but this is almost unanimous in terms of people wanting to move on it.

« Il est important que les forces de l'ordre disposent des outils nécessaires pour enrayer les activités criminelles de façon précoce, souligne Mme Hughes Anthony. Il est prioritaire de faire en sorte que le vol d'identité soit une infraction prévue par la loi — un véritable crime — au Canada, et nous demandons avec instance à toutes les parties de collaborer étroitement et d'adopter cette loi rapidement. »

Mme Hughes a conclu en disant :

« Ces mesures législatives, présentées par le ministre Nicholson, sont une action concrète dans la lutte contre le vol d'identité. Nous applaudissons et soutenons les efforts qu'il déploie pour protéger les Canadiens. »

Monsieur le ministre, je sais que ce projet de loi a été très bien accueilli par les parties intéressées, ce qui est évident. À votre avis, est-ce que le projet de loi a bien été reçu par les Canadiens en général?

M. Nicholson : J'ai reçu de bons commentaires, sénateur Wallace. Encore une fois merci d'avoir introduit ce projet de loi au Sénat. Les Canadiens savent qu'il s'agit d'un problème croissant. J'ai moi-même été victime d'un vol d'identité à un point tel que des renseignements de ma carte de crédit ont été transférés à quelqu'un à Calgary. C'est un point qui me touche, mais la dame qui m'a appelé pour m'informer ne savait pas qui j'étais ni quel lien j'avais avec ce dossier. Lorsqu'elle m'a appelé à la maison pour me parler, elle a dit « Je voulais vous dire que c'est un problème croissant au Canada. » Ce à quoi j'ai répondu « Vous n'avez aucune idée à quel point je suis impliqué dans ce sujet, mis à part le fait que vous m'appelez. »

Je suis allé à Montréal à quelques reprises, et j'ai discuté avec des gens des organismes d'application de la loi qui m'ont dit des choses, que j'avais déjà entendues dans d'autres communautés, à l'effet que les infractions deviennent de plus en plus sophistiquées et que les lois doivent maintenant rattraper le progrès. Nos lois pénales ont été écrites à un moment où l'on pensait que tous les crimes étaient limités au Canada. Cependant, les crimes ne sont plus limités au Canada. Souvent, les renseignements sont transférés dans une fraction de seconde à l'extérieur du pays. En fait, la production de cartes de crédit illégales ou autre mauvaise utilisation des renseignements identificateurs de personne sont souvent faites à l'extérieur du Canada. Nous avons ces lacunes dans la loi qui permettent à ces gens de recueillir des renseignements et de ne pas être poursuivis à cause de ces lacunes dans la loi.

C'est un problème que nous avons toujours eu, franchement, avec le Code criminel de ce pays. Il ne s'agit pas uniquement de sévir face au crime. La plupart de nous voulons le faire ou croyons que c'est important. Un tel projet de loi sert fondamentalement à combler les lacunes qui existent dans le Code criminel. C'est quelque chose que nous devons faire et je crois que c'est important. Je n'ai reçu que des commentaires positifs au sujet de ce projet de loi. Je ne peux en dire autant au sujet de toutes les lois. En général, je reçois de bons commentaires, mais rien à comparer à ce dossier-ci où la réponse est unanime et les gens veulent aller de l'avant.

I cannot say we are the only country in the world not to have this, or the western industrialized countries. The Europeans have a slightly different take on this. Certain legislation in certain European countries is focused on people's financial loss, but it is not just a financial loss when people steal your identity. There are other components to that. I certainly encourage my European or G8 colleagues to look at the whole area and expand people's protection.

Senator Wallace: We all see the changing times we are in and this new reality that is upon us. Every one of us receives mail at home. I know that nothing that comes into my house with my name or address on it goes into the garbage until it goes through the shredder. We all live in fear. That is a recent phenomenon for most of us. In that regard, my sense is that a sense of urgency and timeliness exist to move this bill into law. I am wondering if you would care to comment on that sense of urgency.

Mr. Nicholson: I believe that this is universally welcome to the extent that people focus on this. People are more aware of the challenges with respect to identity and identity theft and how easy that is. At the press conference you and I attended, it was estimated that it is a $2-billion-a-year problem in this country. This is huge. We know that with some of these technological crimes it gets worse. It levels off. Increasing numbers of people become involved in this, particularly if there is a perception that a gap exists in Canadian law. It is incumbent upon us all to move on this. I would like to see it moved through and receive Royal Assent by the end of the session.

Senator Baker: Welcome, minister. When the bill was originally introduced into the House of Commons last year or the year before, it encountered stiff opposition in relation to the shenanigans of the committee examining it, and it died in the committee. I can give you assurances that there will be no such shenanigans here. We will judge the bill on its merits and listen to the witnesses, which they did not do in the House of Commons. That is why you have now introduced it into the Senate first. You are getting sober second thought in the first place without waiting for it.

Senator Angus: Without thinking.

Senator Baker: That was Senator Angus who said, "Without thinking."

I will ask a few questions that I am sure will concern the witnesses who will be appearing before this committee as we examine the bill.

Bill S-4, under the heading "Official Documents," defines "identity document" in proposed new subsection 56.1(3) as follows:

Je ne peux pas dire que nous sommes le seul pays au monde ou même parmi les pays industrialisés occidentaux qui n'ayons pas ce type de loi. Les Européens ont une approche quelque peu différente. Certaines des lois dans certains pays européens sont axées sur les pertes financières des victimes, mais il ne s'agit pas uniquement de pertes financières lorsqu'une personne vole votre identité. Il y a d'autres éléments. J'encourage très certainement mes collègues européens ou membres du G8 à se pencher sur la question et à étendre la protection de leurs citoyens.

Le sénateur Wallace : Nous sommes tous témoins de notre époque changeante et de cette nouvelle réalité qui nous entoure. Tout le monde reçoit du courrier à la maison. Je sais que chez moi aucune pièce de courrier portant mon nom et mon adresse et qui entre dans ma maison ne va aux poubelles avant d'être passé par la déchiqueteuse. Nous vivons tous dans la peur. C'est un phénomène tout récent pour la plupart d'entre nous. À cet égard, je crois qu'il y a un sentiment d'urgence et d'actualité qui pousse à faire avancer ce projet de loi et à le rendre loi. Je me demande si vous voudriez ajouter quelques mots au sujet de l'urgence de la situation.

M. Nicholson : Je crois que c'est universellement reconnu et que les gens s'y intéressent. Tout le monde est conscient des changements relatifs à l'identité et au vol d'identité ainsi qu'à la facilité de ce crime. Il a été dit à la conférence de presse à laquelle vous et moi avons participé que le problème au pays était évalué à une perte de 2 milliards de dollars par année. C'est énorme. Et nous savons que dans certains crimes technologiques c'est encore pire. Mais cela se stabilise. Le nombre de personnes impliquées augmente, d'autant plus que la loi canadienne est réputée comporter des lacunes. Il nous incombe de faire avancer le dossier. J'aimerais qu'il reçoive la sanction royale d'ici la fin de la session.

Le sénateur Baker : Bienvenue, monsieur le ministre. Lorsque le projet de loi a été introduit à la Chambre des communes l'année dernière ou l'année d'avant, il a été accueilli par une vive opposition et les manigances du comité qui l'étudiait, ce qui a eu pour effet de faire mourir le projet au feuilleton. Je peux vous assurer qu'il n'y aura aucune manigance de la sorte ici. Nous jugerons le projet de loi sur son fond et nous écouterons les témoins, ce qui n'a pu avoir lieu à la Chambre des communes. C'est pourquoi vous l'avez introduit au Sénat en premier. Vous allez avoir un second examen objectif en premier lieu et sans attendre.

Le sénateur Angus : Sans réfléchir.

Le sénateur Baker : C'est le sénateur Angus qui a dit « Sans réfléchir. »

Je vais poser quelques questions qui vont certainement intéresser les témoins qui se présenteront au comité pendant l'étude de ce projet de loi.

Sous le titre « Documents officiels » du projet de loi S-4 on définit « pièce d'identité » en vertu du nouveau paragraphe 56.1(3) de la façon suivante :

For the purposes of this section, "identity document" means a Social Insurance Number card, a driver's licence, a health insurance card, a birth certificate, a passport as defined in subsection 57(5), a document that simplifies the process of entry into Canada, a certificate of citizenship, a document indicating immigration status in Canada or a certificate of Indian status, issued or purported to be issued by a department or agency of the federal government or of a provincial government, or any similar document issued or purported to be issued by a foreign government.

That is it; no other documents are considered to be an identity document. Therefore, a person looking at this, on the face of it, would ask why you are restricting identity documents, under the general heading "Official Documents," to a restricted list that will not take into account any other identity document that may be of use.

Mr. Nicholson: This carves out a special section. It is not exclusive in that there are no other provisions directed toward identity information or some type of identity card. It creates a specific offence with respect to government-related documents. There is a very low threshold that a person who simply possesses one of these items without lawful excuse is guilty of an offence. We think it would go too far if we said, of every bit of information that could possibly be gathered, that it would be an offence, in and of itself, to possess that. With government documentation, if you do not have a lawful excuse why you have other people's passports, for example, in your possession, we carved out a specific offence.

Your question is whether the list is complete. It looks to be a fairly extensive list of government documentation. Let us know if you can think of some other government documentation. We have carved out this specific offence, but it does not mean, nor should we give the impression, that the rest of the bill does not talk about the transfer of all types of personal information not directly connected with government documentation.

Senator Baker: Senator Wallace referenced people being concerned about identity theft and receiving items in the mail. A large portion of this bill deals with the mail. I do not know if you have turned your mind to this. The identification of a social insurance number as an identity document has been decided by the Personal Information Protection and Electronic Documents Act, PIPEDA. Judgments are given every week by the Privacy Commissioner as to whether federal institutions or institutions that come under federal jurisdiction are breaking the law with the use and release of personal information.

Mr. Nicholson: That is correct.

Senator Baker: For example, the banks came under fire. It was judged to be an offence under the act to use a social insurance number to identify someone on their documents.

Pour l'application du présent article, « pièce d'identité » s'entend de la carte d'assurance sociale, du permis de conduire, de la carte d'assurance maladie, du certificat de naissance, du passeport au sens du paragraphe 57(5), de tout document simplifiant les formalités d'entrée au Canada, du certificat de citoyenneté, de tout document indiquant un statut d'immigration au Canada ou du certificat du statut d'indien, délivré ou paraissant délivré par un ministère ou un organisme public fédéral ou provincial, ou de tout autre document semblable délivré ou paraissant délivré par un gouvernement étranger.

C'est tout. Aucun autre document n'est considéré comme une pièce d'identité. Par conséquent, une personne qui lit cet article, vous demanderait pourquoi vous limitez les pièces d'identité, sous le titre général de « documents officiels », à une liste qui ne tiendra pas compte de tout autre document d'identité qui pourrait être utilisé.

M. Nicholson : Ceci crée un article spécial. Il n'est pas exclusif dans ce sens qu'aucune autre disposition ne traite spécifiquement de renseignements identificateurs ou de tout type de carte d'identité. Il crée une infraction précise concernant les documents gouvernementaux. Il impose un seuil très bas pour les personnes qui ont en leur possession certains de ces articles sans excuse légitime et qui deviennent alors coupables d'infractions. Nous pensons que ce serait allé trop loin de dire que la possession de tout élément d'information qui peut être recueilli serait une infraction. Avec les documents gouvernementaux, si vous n'avez pas d'excuses légitimes pour avoir en votre possession le passeport de quelqu'un par exemple, nous avons créé une infraction précise.

Vous voulez savoir si la liste est complète. Ça semble être une liste passablement longue de documents gouvernementaux. Veuillez nous faire connaître tout autre document gouvernemental auquel vous pourriez penser. Nous avons indiqué nommément ces infractions particulières, mais cela ne signifie pas — et il faut bien se garder d'avoir une telle impression — que le reste du projet de loi passe sous silence la transmission de tout type de renseignements personnels n'ayant pas de lien direct avec de la documentation gouvernementale.

Le sénateur Baker : Le sénateur Wallace a parlé des personnes qui sont préoccupées par le vol d'identité et qui reçoivent des articles par la poste. Une bonne partie du projet de loi porte sur le courrier. L'indication d'un numéro d'assurance sociale comme pièce d'identité a été décidée aux termes de la Loi sur la protection des renseignements personnels et les documents électroniques, la LPRPDE. Chaque semaine, le Commissaire à la protection de la vie privée rend des jugements sur la question de savoir si des institutions fédérales ou des institutions qui relèvent du pouvoir fédéral commettent une infraction quand elles utilisent ou communiquent des renseignements personnels.

M. Nicholson : C'est exact.

Le sénateur Baker : Les banques, par exemple, ont été visées. Un jugement rendu à cet égard a établi que c'était une infraction au sens de la loi d'utiliser le n° d'assurance sociale pour identifier une personne sur leurs documents.

I am sure that we will have people appearing before the committee who will say that the government uses our social insurance numbers to identify us as senior citizens. When we get a senior citizens card — which you will receive one of these days, like I did a few years ago — you will see that the identity number is your social insurance number. When someone receives Old Age Security in Canada or Canada Pension in the mail — not registered mail — it includes their name, address and social insurance number, their identity, and access code to the Internet to access their account.

Have you turned your mind to assembling information to examine government violations in this area and to say that to various government departments that they cannot be sending peoples' social insurance numbers through the mail or use it as an identity?

Mr. Nicholson: You are referencing the PIPEDA, but the bill we have before us is not directed toward that. That is not to say that it is not an important subject, and privacy concerns are always a concern for government. This bill is confined specifically to the misuse of information. You will notice that each section, as you go through clause-by-clause consideration, always has a disclaimer: without lawful excuse or without lawful authorization. People using information for a legitimate purpose are specifically excluded in all cases throughout this bill. It specifically targets organized crime. That is who they tell me is involved with this activity. Organized crime syndicates are collecting this information, shipping it outside the country and using it for illegal purposes.

That issue is an interesting subject for a different bill or another time, but this bill is not directly making any amendments to PIPEDA or anything else. This bill is specifically designated to target the misuse of people's information for criminal purposes.

Senator Baker: Finally, you referenced this question in your opening address. It is a proposed new section of the bill that may concern certain witnesses who may appear before the committee. The proposed new section 368(1)(*c*) says that if you transmit another person's identity information or have it in your possession, "knowing that or being reckless" as to whether the information will be used to commit a crime.

Are you concerned that the expression "being reckless" would perhaps lead to unjustified prosecutions under this act?

Mr. Nicholson: I do not think so. I looked at that when we introduced this approximately one year ago. We want to get that individual who says that he or she did not pay any attention at all and was only collecting information and sending it to a good friend who happened to be south of the border, that he or she was only helping out.

Je suis sûr que certaines personnes qui comparaîtront devant le comité diront que le gouvernement utilise nos n^{os} d'assurance sociale pour nous identifier comme personnes âgées. Quand vous recevrez une carte d'identité de personnes du troisième âge — vous en recevrez une un de ces jours, comme j'ai en reçu une il y a quelques années — vous verrez que le n^{o} d'identité est votre n^{o} d'assurance sociale. Sur les documents de prestations de la Sécurité de la vieillesse ou du Régime de pensions du Canada qui sont envoyés par la poste — pas par courrier recommandé — on indique le nom, l'adresse et le n^{o} d'assurance sociale du destinataire, son identité et le code d'accès Internet permettant d'avoir accès à son compte.

Avez-vous pensé à réunir de l'information en vue d'examiner les violations commises par le gouvernement à cet égard et pour informer les divers ministères qu'ils ne peuvent envoyer par la poste ni utiliser comme moyen d'identité le n^{o} d'assurance sociale des citoyens?

M. Nicholson : Vous parlez d'un aspect de la LPRPDE, mais le projet de loi que nous étudions ne porte pas là-dessus. Ce n'est pas que ce ne soit pas un sujet important et le gouvernement a toujours à cœur tout ce qui concerne la protection des renseignements personnels. Le projet de loi que nous examinons en ce moment porte spécifiquement sur la mauvaise utilisation de l'information. Pendant votre étude article par article, vous remarquerez qu'il y a toujours une mise en garde : sans excuse légitime ou sans autorisation légitime. Tout au long du projet de loi, les personnes qui utilisent l'information de façon légitime sont spécifiquement exemptées dans tous les cas. La loi vise spécifiquement la criminalité organisée. C'est ainsi qu'on indique qui prend part à ce genre d'activité. Les organisations criminelles collectent ce genre de renseignements, les transmettent à l'extérieur du pays et les utilisent à des fins criminelles.

Cette question constitue un intéressant sujet pour un autre projet de loi à présenter à un autre moment, mais le projet de loi que nous examinons en ce moment n'a pas pour objectif direct d'apporter des modifications à la LPRPDE ou quoi que ce soit d'autre. Son objet est de cibler spécifiquement l'utilisation de l'information concernant les citoyens à des fins criminelles.

Le sénateur Baker : Enfin, vous avez fait mention de cette question dans votre allocution d'ouverture. Il s'agit d'un projet d'article nouveau de la loi qui pourrait concerner certains témoins appelés à comparaître devant le comité. Dans le projet de nouvel alinéa 368(1)*c*), il est question de toute personne qui transmet des renseignements identificateurs sur une autre personne ou qui les a en sa possession et qui les transmet « ne se souciant pas de savoir » si cette information servira à commettre une infraction.

Ne craignez-vous pas que l'expression « ne se souciant pas », la notion d'insouciance, ouvre peut-être la porte à des poursuites injustifiées aux termes de la loi?

M. Nicholson : Je ne crois pas. J'ai examiné cet aspect lorsque j'ai présenté le projet de loi il y a environ un an. Nous visons les personnes qui affirment ne pas avoir fait attention et qu'elles ne faisaient que collecter de l'information et qu'elles faisaient parvenir à un bon ami au sud de la frontière, simplement pour rendre service.

We have to get that individual who was reckless in assembling people's information and shipping it somewhere to someone else for an illegal purpose. He or she is a part of the chain; and we cannot have those people saying that they do not think about these things and only like to gather people's information. We have to get all people who are reckless or intend to participate in a criminal enterprise.

The Chair: Is there not a difference between someone who is reckless and someone who has criminal intent and criminal associations?

Mr. Nicholson: The term "reckless" is use a number of times in the Criminal Code. People who conduct themselves in a reckless manner can find themselves subject to criminal liability. We are applying it in this case as well.

The Chair: I think that is the area that Senator Baker may wish to resume on the second round.

Joanne Klineberg, Counsel, Criminal Law Policy Section, Department of Justice Canada: It is true that the term "recklessness" is used in a few sections of the Criminal Code. It has been interpreted by the courts to mean a standard that is only slightly less than actual knowledge or intent. The courts say that "recklessness" means awareness of a substantial risk that something would happen, actual subject of the awareness of the risk that it would happen and a decision to proceed with the behaviour nonetheless.

It is somewhat more than a mere inadvertence or not turning your mind to it. You actually must perceive the risk. It actually would be even more than gross negligence. Gross negligence would be a case of inadvertence that rises to the level of being very dangerous. Recklessness would require proof of a subject of awareness of the risk on the part of the accused, but not knowledge necessarily, only knowledge of the risk.

Senator Milne: Minister, I am made to feel more comfortable by proposed new subsection 56.1(2) that says:

> For greater certainty, subsection (1) does not prohibit an act that is carried out . . .
>
> (b) for genealogical purposes; . . . .

I am the family genealogist, but this line of questioning by Senator Baker has the hair on the back of my neck standing up. I regularly send personal information about people who contact me because they want more information about the Milne clan, and I send it to them. I have absolutely no idea how they are going to use it. They tell me they are genealogists. Of course, they probably are, but nevertheless, I might be being reckless.

Nous voulons atteindre cette personne qui a fait preuve d'insouciance en réunissant des renseignements personnels et en les transmettant ailleurs, à une personne qui en fera un usage illégal. Il ou elle fait partie de la chaîne; et nous ne pouvons pas admettre que ces personnes affirment ne pas y avoir pensé et qu'elles aiment tout simplement recueillir des renseignements personnels. Nous voulons atteindre les personnes qui font preuve d'insouciance ou qui ont l'intention de participer à une entreprise criminelle.

La présidente : Est-ce qu'il n'y a pas une différence entre une personne qui fait preuve d'insouciance et une personne qui a une intention criminelle ou des liens avec une organisation criminelle?

M. Nicholson : Le mot « insouciance » revient un certain nombre de fois dans le Code criminel. Les gens qui font preuve d'insouciance dans leur façon d'agir peuvent être tenus criminellement responsables de leurs actes. C'est cette logique que nous appliquons ici.

La présidente : Je pense que c'est l'aspect sur lequel le sénateur Baker voudrait revenir pendant la deuxième série.

Joanne Klineberg, avocate, Section de la politique en matière de droit pénal, ministère de la Justice du Canada : Il est exact de dire que le mot « insouciance » est utilisé dans quelques articles du Code criminel. Les tribunaux l'interprètent dans un sens qui le situe légèrement en dessous de la connaissance de cause ou de l'intention. Pour les tribunaux, le mot « insouciance » renvoie à la conscience de l'existence d'un risque important que quelque chose se produise, la conscience subjective chez une personne de l'existence d'un risque qu'il se produise quelque chose et qui décide néanmoins de passer à l'acte.

C'est un peu plus que la simple inadvertance ou que le fait de ne pas y penser. Il doit y avoir de la part de la personne concernée une perception du risque. Ce serait même plus fort que de l'imprudence grave. L'imprudence grave, ce serait l'inadvertance portée à un niveau tel qu'elle en devient très dangereuse. Pour conclure à l'insouciance, il doit y avoir la preuve d'une conscience subjective de l'existence d'un risque chez l'accusé, mais pas forcément la connaissance, seulement la connaissance du risque.

Le sénateur Milne : Monsieur le ministre, le nouveau paragraphe 56.1(2) qui est proposé me met plus à l'aise; on y lit ce qui suit :

> Il est entendu que le paragraphe (1) ne prohibe pas un acte qui a été accompli :
>
> *b*) à des fins généalogiques.

Je suis la généalogiste familiale, mais les questions que le sénateur Baker pose me font dresser les cheveux sur la tête. J'envoie régulièrement des renseignements personnels au sujet de personnes qui communiquent avec moi pour obtenir des renseignements sur le clan Milne, et je les leur envoie. Je n'ai pas la moindre idée de ce qu'ils feront de cette information. Ils me disent être des généalogistes. Naturellement, c'est probablement le cas, mais il se pourrait que je fasse néanmoins preuve d'insouciance.

Ms. Klineberg: Unless some circumstances could be demonstrated that would have given rise in your own mind of a serious risk that someone would use the information for criminal purposes, you would not be being reckless. If you failed to turn your mind to the question at all, or if you just assumed that the purpose will be lawful, that would not count as recklessness under a criminal law standard.

Senator Milne: Let us hope that gets me off the hook sometime in the future.

Following from what Senator Baker was saying, current Canadian law imposes limits on how long organizations engaged in commercial activities can retain personal information. It is not to be stored in perpetuity by these organizations. I understand that the Privacy Commissioner and the BC Freedom of Information and Privacy Association have noted that the risk of identity theft in the private sector would be significantly reduced if this law was actually obeyed by organizations — specifically, the law on personal information in section 4 of the PIPEDA.

I suspect from your answers that you agree with me, but why are we not doing more right now to have the government do more to enforce the laws that already exist that would help with this issue considerably?

Mr. Nicholson: The government is concerned about protecting Canadians from breaches involving loss of personal information stored by companies. Again, the legislation I have is not directed toward the Personal Information Protection and Electronic Documents Act. You are right. There is information. There is legislation with respect to privacy, and it should be enforced, of course, by all law enforcement agencies. All government agencies should be very careful.

We are not dealing today with amendments to that particular act. We are dealing with criminal activity, namely, people assembling information for criminal purposes or the theft of people's personal information. It was not meant to be an amendment to the PIPEDA.

Senator Milne: I know that. If we already have one act that is unenforceable, why are we bringing up another act that I strongly suspect will be unenforceable as well?

Mr. Nicholson: I do not agree that PIPEDA is unenforceable. It can and should be enforced, and people should comply with the provisions and be careful.

We are always looking at better ways to protect people's personal information that is held by the government or the companies. Again, we do not mind addressing these issues. We do not mind looking into them, but this bill is specific to the gaps that are in the Criminal Code with respect to the theft of people's identity.

Senator Milne: Minister, I applaud the purpose behind this act.

Me Klineberg : À moins qu'il soit possible de démontrer l'existence de circonstances qui pouvaient vous faire craindre qu'il y avait un risque grave qu'une personne utilise l'information à des fins criminelles, il ne s'agirait pas d'insouciance de votre part. Si vous avez omis de vous poser la question ou si vous avez simplement présumé que la requête était légitime, il ne s'agirait pas d'insouciance au sens du droit pénal.

Le sénateur Milne : Espérons que cela m'évite d'éventuels ennuis dans l'avenir.

Si j'enchaîne sur ce que disait le sénateur Baker, la loi canadienne actuelle fixe des limites au temps pendant lequel des organisations poursuivant des activités commerciales peuvent conserver des renseignements personnels. Elles ne peuvent les conserver dans leurs archives à perpétuité. Je crois comprendre que le Commissaire à la protection de la vie privée et la BC Freedom of Information and Privacy Association ont souligné que le risque de vol d'identité dans le secteur privé serait considérablement atténué si les organisations se conformaient effectivement à cette loi, et en particulier à l'article 4 de la LPRPDE.

Vos réponses me donnent à penser que vous êtes d'accord avec moi, mais qu'attend le gouvernement pour prendre des mesures pour faire appliquer les lois qui existent déjà et qui seraient d'une très grande utilité relativement à la question dont nous parlons?

M. Nicholson : Le gouvernement a une véritable volonté de protéger les Canadiens contre les infractions reliées à la perte de renseignements personnels conservés par les entreprises. Encore une fois, la loi que nous examinons ne concerne pas la Loi sur la protection des renseignements personnels et les documents électroniques. Vous avez raison. Il s'agit de renseignements. Il existe une loi qui concerne la protection des renseignements personnels et il faudrait naturellement que tous les organismes d'application de la loi la fassent respecter. Tous les organismes gouvernementaux doivent être très vigilants.

Aujourd'hui, nous ne nous occupons pas d'amendements à cette loi particulière. Nous nous penchons sur la question des activités criminelles, à savoir celles de personnes qui recueillent des renseignements à des fins criminelles, ou le vol de renseignements personnels. Il n'était pas question d'en faire une modification de la LPRPDE.

Le sénateur Milne : Je le sais très bien. S'il existe déjà une loi qui est inexécutable, pourquoi en présenter une autre dont je doute fortement qu'elle soit davantage exécutable?

M. Nicholson : Je ne suis pas d'accord pour dire que la LPRPDE est inexécutable. Elle peut et elle doit être appliquée et tous doivent se conformer à ses dispositions et faire attention.

Nous sommes toujours à la recherche de meilleures façons de protéger les renseignements personnels que détiennent le gouvernement ou les entreprises. Une fois encore, nous n'avons rien contre l'idée de nous pencher sur ces questions. Nous n'avons rien contre l'idée de les examiner, mais le projet de loi que nous étudions maintenant a pour objet spécifique de combler les lacunes que présente le Code criminel en matière de vol d'identité.

Le sénateur Milne : Monsieur le ministre, j'applaudis à l'intention de la loi.

Mr. Nicholson: Good.

Senator Milne: I also note that almost every one of the bills that we see coming down the pike toward this committee have mandatory minimum sentences set out in them, but not in this bill.

Mr. Nicholson: I always try to keep an open mind, if you are suggesting an amendment.

Senator Milne: Why is that, minister? Is this just an oversight, or do you intend to bring in another bill to correct that?

Mr. Nicholson: We are always looking for guidelines, and that is our responsibility, senator. You might ask why we are putting maximum sentences here; it is because we give guidance to the courts. On each of these offences, we do give guidance, and we put maximums.

I remember years ago, as a member of the standing committee on justice, one of my colleagues asked why the maximum was only five years and suggested giving judges the ability because they might find it is worth seven or ten years.

We have to judge these in connection with other sections of the Criminal Code, and that is why the maximum on that particular offence was only five years, even though I had colleagues in my own party who thought it should be seven or ten years. Again, that is our job as parliamentarians, to give maximums. Sometimes we give minimums. We give guidance to the courts. I think it is a good way to handle it.

Senator Milne: It is minimums I am talking about.

Mr. Nicholson: We are not putting in any minimums.

Senator Milne: Have you any evidence whatsoever that mandatory minimums work?

Mr. Nicholson: I hear it all the time, senator, that we have to send the correct message out. We have a bill directed at people who, for instance, are bringing drugs into this country and are involved almost exclusively with organized crime, namely, criminal gangs bringing drugs into this country. In that case, we have mandatory jail terms because we want to send out a clear message that says that people bringing drugs into the country are in the business of destroying Canadian lives. We have to send out a message. We give that guidance to the courts. We do not have them on all bills and not on the bill before you. However, if you look at the penalties in it, they are reasonable and give the guidance that is our responsibility to give the courts.

M. Nicholson : Bon.

Le sénateur Milne : Je note également que presque tous les projets de loi qui sont soumis à l'examen de notre comité sont assortis de peines minimales obligatoires qui y sont précisées, ce qui n'est pas le cas avec le présent projet de loi.

M. Nicholson : Je suis disposé à examiner toute suggestion d'amendement que vous pourrez faire.

Le sénateur Milne : Pourquoi cette absence, monsieur le ministre? S'agit-il simplement d'une omission, ou bien avez-vous l'intention de présenter un autre projet de loi pour la corriger?

M. Nicholson : Nous cherchons toujours à indiquer des lignes directrices, c'est notre responsabilité, madame le sénateur. Vous voulez peut-être savoir pourquoi nous indiquons des peines maximales; c'est pour guider les tribunaux. Pour chacune des infractions indiquées, c'est ce que nous faisons, guider les tribunaux en précisant des peines maximales.

Je me rappelle il y a quelques années, alors que je siégeais à titre de membre du Comité permanent de la justice, qu'un de mes collègues a demandé pourquoi le maximum n'était que de cinq ans, et il avait suggéré de laisser au juge le soin de déterminer si l'infraction ne valait pas à son auteur une peine d'une durée de 7 ou de 10 ans.

Nous devons examiner des questions de ce genre en fonction d'autres articles du Code criminel, et c'est là la raison pour laquelle le maximum avait été fixé à cinq ans dans le cas de cette infraction particulière, même si certains collègues de mon propre parti étaient d'avis qu'il aurait fallu le fixer à sept ou 10 ans. Une fois encore, il nous incombe, à titre de parlementaires, de fixer des maximums. Parfois, nous indiquons des minimums. Nous cherchons à guider les tribunaux. Je crois que c'est une bonne façon de procéder.

Le sénateur Milne : C'est bien de minimums que je parle.

M. Nicholson : Nous n'indiquons aucun minimum.

Le sénateur Milne : Avez-vous une preuve quelle qu'elle soit que les peines minimales obligatoires fonctionnent?

M. Nicholson : Madame le sénateur, combien de fois j'ai entendu dire qu'il fallait envoyer un message clair. Il y a une loi qui cible les personnes qui, par exemple, importent des drogues au Canada et qui sont reliées presque exclusivement au crime organisé, à savoir les bandes criminelles qui importent des drogues au Canada. Dans ce cas-là, des peines d'emprisonnement obligatoires sont fixées parce que nous voulons envoyer un message clair, à savoir que les gens qui importent des drogues au Canada s'adonnent à une activité qui détruit des vies de Canadiens. Il faut envoyer un message et nous guidons les tribunaux. Nous ne précisons pas les peines minimales dans tous les projets de loi et nous ne les précisons pas dans le projet de loi devant vous. Mais examinez bien les peines qui y sont indiquées; elles sont raisonnables et elles servent à guider les tribunaux comme il est de notre responsabilité de le faire.

Senator Milne: I notice, Madam Chair, that the minister has not given us any idea whatsoever that mandatory minimums work, and since they are not in this bill, I will subside at this point.

Senator Nolin: We will have a bill soon that will discuss exactly that.

The Chair: There are a number, I do believe.

Senator Nolin: We will be privileged to have the minister come back.

The Chair: I have a question on this line, minister, that may surprise you, coming from someone who sits on our side of the chamber, and it has to do with maximum sentences. As an example, the maximum for stealing anything sent by post is ten years, but the maximum for impersonating a police officer is only five years.

Ms. Klineberg: Sometimes when we amend the Criminal Code, anomalies appear. In this particular case, we currently have section 356 of the Criminal Code, which provides a number of offences in relation to Canada Post. It does have a ten-year maximum, so as we were adding offences to that existing offence, the decision was made to keep that penalty the same, at ten years.

In relation to impersonating a peace officer, that currently is a summary conviction offence. It is being hybridized in this bill, with the penalty being increased to five years. As the minister has suggested, it is sometimes a challenge to determine what maximum penalties should be and what the nature of the guidance you want to give the courts should be. If you look at the elements of that offence, it is one which, relative to the other identity theft offences that were created, we thought would be consistent.

Senator Bryden: With respect to the difference of the penalties, it is interesting to me that in proposed new section 368.1 of the bill, everyone is guilty of an indictable offence and liable to imprisonment for a term of not more than 14 years if various things happen, which are happening all through this.

Why was this one chosen to have a maximum of 14 years, while another one has a maximum of 10, and the others have maximums of 5? I am a great believer that it does not matter what the maximum is but whether you get caught or not, and that is the difficult part.

Mr. Nicholson: We tried to make them consistent with sections already in the Criminal Code. There are those, senator, who have said from time to time that what we should do is start from scratch in the Criminal Code, and try to reconcile every section of the Criminal Code.

Le sénateur Milne : Je note, madame la présidente, que le ministre ne nous a pas donné la moindre idée de l'efficacité des peines minimales obligatoires, et comme il n'en figure aucune dans le projet de loi, je n'en dirai pas davantage à ce stade-ci.

Le sénateur Nolin : Un projet de loi sera présenté prochainement qui portera exactement sur cet aspect.

La présidente : Il y en aura un certain nombre, je crois.

Le sénateur Nolin : Nous aurons l'honneur d'accueillir de nouveau le ministre.

La présidente : J'ai une question à poser à ce sujet, monsieur le ministre; cela pourra vous surprendre de la part d'une personne qui siège du même côté que vous à la Chambre. C'est au sujet des peines maximales. À titre d'exemple, la peine maximale pour avoir volé un article envoyé par la poste est de 10 ans, mais elle n'est que de 5 ans dans le cas d'une personne qui se serait fait passer pour un agent de police.

Mme Klineberg : Parfois, des anomalies surviennent lorsque nous modifions le Code criminel. Dans ce cas en particulier, l'article 356 du Code criminel porte sur un certain nombre d'infractions liées à Postes Canada. L'article prévoit un emprisonnement maximal de dix ans, alors comme nous ajoutions des infractions à l'infraction en question, nous avons décidé de garder la même pénalité, à savoir dix ans d'emprisonnement.

En ce qui concerne le fait de prétendre faussement être un agent de la paix, il s'agit actuellement d'une infraction punissable par voie de déclaration sommaire de culpabilité. Il s'agit d'une hybridisation dans le présent projet de loi, et la pénalité est augmentée à cinq ans d'emprisonnement. Comme le ministre l'a laissé entendre, il est parfois difficile de déterminer quelles pénalités maximales doivent être imposées et la nature de l'orientation que l'on veut donner aux tribunaux. Si on examine les éléments de cette infraction, nous pensions que cela serait cohérent par rapport aux autres infractions liées aux vols d'identité.

Le sénateur Bryden : En ce qui concerne la différence entre les pénalités, je trouve intéressant que dans le nouvel article proposé 368.1 du projet de loi, tout le monde est coupable d'un acte criminel passible d'un emprisonnement maximal de 14 ans dans certaines circonstances, qui surviennent dans ce contexte.

Pourquoi cette infraction est-elle passible d'une peine maximale de 14 ans, alors qu'une autre infraction est passible d'une peine maximale de 10 ans d'emprisonnement, et que d'autres infractions sont passibles d'une peine maximale de 5 ans? Je crois fermement qu'il n'est pas important de savoir quelle est la peine maximale. Ce qui est important, c'est de savoir si on se fera prendre, et c'est là que ça se corse.

M. Nicholson : Nous essayons d'assurer une cohérence avec les articles qui se trouvent déjà dans le Code criminel. Il y a des gens, monsieur le sénateur, qui ont dit parfois que ce que nous devrions faire serait de recommencer à zéro en ce qui concerne le Code criminel, et essayer de faire concorder tous les articles du Code criminel.

You can appreciate that getting even minor amendments sometimes can be a challenge. I do not have the nerve to tackle the question of revising the whole Criminal Code. Again, making it consistent with the sections that we are placing it in sometimes guides us on what those would be. As you point out, we seldom see the maximum sentences being given out, but they are there as guidelines.

Senator Joyal: Minister, if you allow me, as part of my opening remarks, I would like to draw your attention to one of the honourable senators around this table, our colleague Senator Angus, who has been granted the merit medal of the Quebec Bar this year.

Senator Baker: Well deserved.

Senator Angus: Thank you.

Senator Joyal: Minister, my first question is in relation to clause 11 of the bill, which amends subsection 738(1) of the Criminal Code, entitled "Restitution." This is a very important amendment to the code because it adds the principle of dommages et intérêts, at least in the French version, and that is where I was struck by the concept of dommages et intérêts, which is, of course, mainly a civilian notion.

With the proposed changes, we would have to read subsections 738(1)(*a*), (*b*), (*c*) and (*d*) concurrently or in isolation. If I read subsection 738(1)(*a*), maybe I should say that it is the damages that could be granted by the court when the court has recognized that the person is responsible for the act.

Therefore, subsection 738(1)(*a*) would allow a judge to grant repair in the case of loss of property. Suppose that someone stole the identity of someone and that leads to the loss of the house; we know that has happened. There was a scheme among real estate agents and so forth recently. You might have heard of it.

Mr. Nicholson: Yes.

Senator Joyal: Then if I read section 738(1), a person who is found guilty could be fined by the court the amount of the damages that are equivalent to the loss of the property, which would be the house in that case.

Then you add proposed new subsection 738(1)(*d*), clause 11 of your bill, which reads that the judge can grant damages equivalent to the cost of re-establishing their identity. In other words, it would be the cost incurred in getting a new credit card, a new passport and so forth.

I applaud that, even though it raises a very fundamental question, in my opinion, which is to introduce the notions of dommages et intérêts in the Criminal Code. It is a very fundamental change to introduce that into the code. Since you do that, to compensate the person for the cost incurred to re-establish his or her identity, why do you not also cover the other costs that a person might have incurred? For instance, someone might be responsible for all sorts of expenses that have

Vous pouvez constater qu'il peut être difficile parfois ne serait-ce que d'apporter des modifications mineures. Je ne me sens pas disposé à attaquer la question de la révision de l'ensemble du Code criminel. De nouveau, le fait de rendre le tout cohérent avec les articles que nous ajoutons peut parfois nous guider sur ce que ces articles devraient être. Comme vous le signalez, les sentences maximales sont rarement imposées, il s'agit plutôt d'un principe directeur.

Le sénateur Joyal : Monsieur le ministre, si vous me permettez, dans le cadre de mes remarques préliminaires, j'aimerais attirer votre attention sur un des sénateurs présents à cette table, notre collègue le sénateur Angus, qui a reçu l'ordre du mérite du Barreau du Québec cette année.

Le sénateur Baker : C'était tout à fait mérité.

Le sénateur Angus : Merci.

Le sénateur Joyal : Monsieur le ministre, ma première question porte sur l'article 11 du projet de loi, qui modifie le paragraphe 738(1) du Code criminel intitulé « Dédommagement ». Il s'agit d'une modification très importante au Code, car la clause renforce le principe de dommages et intérêts, à tout le moins dans la version française, et c'est dans ce cas que j'ai été frappé par le concept de dommages et intérêts, qui est, bien entendu, une notion de nature civile.

Compte tenu des modifications proposées, nous devrions lire les alinéas 738(1)*a*), *b*), *c*) et *d*) de façon simultanée ou séparée. Si je lis l'alinéa 738(1)*a*), je devrais peut-être dire qu'il s'agit des dommages qui pourraient être accordés par la Cour lorsque celle-ci reconnaît qu'une personne est responsable de l'acte.

Par conséquent, l'alinéa 738(1)*a*) permettrait à un juge d'accorder réparation dans le cas d'une perte de biens. Supposons qu'une personne vole l'identité d'une autre personne et que cette situation mène à la perte de la maison de la victime. Nous savons que ce genre de situation est déjà survenu. On a vu une telle situation impliquant des agents immobiliers récemment. Vous en avez probablement entendu parler.

M. Nicholson : Oui.

Le sénateur Joyal : Et si je lis le paragraphe 738(1), une personne trouvée coupable peut recevoir une amende imposée par la Cour couvrant le montant des dommages équivalant à la perte des biens, à savoir la perte de la maison dans ce cas.

Puis on ajoute le nouvel alinéa proposé 738(1)*d*), l'article 11 de votre projet de loi, qui indique que le juge peut accorder des dommages équivalant au coût du rétablissement de son identité. Autrement dit, cela correspondrait aux frais engagés pour obtenir une nouvelle carte de crédit, un nouveau passeport, et cetera.

J'approuve tout cela, même si la situation soulève une question des plus fondamentales, à mon avis, qui est liée à l'introduction des notions de dommages et intérêts dans le Code criminel. Il s'agit d'un changement des plus fondamentaux à introduire dans le code. Comme vous faites cela afin de compenser la personne pour les frais encourus liés au rétablissement de son identité, pourquoi ne couvrez-vous pas aussi les autres frais qu'une personne aurait engagés? Par exemple, une personne peut être

been made on his or her behalf and, of course, the person would find himself or herself open to litigation because of that and not able to be compensated by the person who authors the fraud.

It seems to me that if the principle is good for the loss of property, it should be good for other damages or expenses that the person was led to incur, other monetary losses, because his or her identity has been stolen.

Mr. Nicholson: I believe that would be covered under subsection 738(1)(*a*) of that as well. In your case, the person who has lost the house would be able to be provided for under subsection 738(1)(*a*), so, in a sense, we are adding other expenses that may be collectible.

Senator Joyal: I understand the house is covered by subsection 738(1)(*a*), but the person might have incurred other expenses because his or her identity has been stolen and the person has been found responsible for it.

The Chair: A credit card bill is not property.

Senator Joyal: Property, to me, is a building.

Mr. Nicholson: I will ask Ms. Klineberg to comment on that one, senator.

Ms. Klineberg: It becomes a difficult question of how remote and how far removed are the full set of consequences of the crime. The direct costs associated with rehabilitating your identity would be covered. Whether or not additional costs, such as being involved in a civil litigation action, should be covered is a very difficult aspect to balance with respect to how far you want to use the criminal law restitution power to deal with what is essentially a civil law matter. There was some concern that if we allowed restitution of many things that require a civil court to engage in a fact-finding process, to balance and measure exactly what the costs were, it would be too onerous for a criminal court in the context of a sentencing hearing to evaluate what those costs are. Those costs, as well, might not be known at the time of sentencing an offender. If there is some sort of civil action where the person has to clear, for instance, a false mortgage that was taken out on their property, it might take quite some time to determine what the true costs of discharging that mortgage would be. They would not necessarily be readily ascertainable at the time of sentencing the offender.

If you notice throughout subsections 738(1)(*a*), (*b*), (*c*) and proposed new subsection (*d*), all of the costs that are recoverable through restitution must be readily ascertainable. The point is that at the time of the criminal trial, the criminal court has to be in a position to be able to concretely say what the costs are in order to be able to order restitution. Once you fall outside those bounds, you are in the domain of civil law and civil restitution.

responsable de toutes sortes de dépenses faites en son nom, et bien entendu, la personne serait amenée à s'engager dans un litige car elle ne sera pas capable de recevoir une compensation de la part de l'auteur de la fraude.

Il me semble que si le principe est bon pour la perte de biens, il devrait aussi l'être pour les autres formes de dommages ou de dépenses que la personne aura engagées, pour les autres pertes monétaires, se rapportant au vol de son identité.

M. Nicholson : Je crois que ce sujet serait couvert par l'alinéa 738(1)*a*). Dans votre cas, la personne qui a perdu sa maison pourrait recourir à l'alinéa 738(1)*a*), et ainsi, nous ajoutons d'autres dépenses qui pourraient être recouvrables.

Le sénateur Joyal : Je comprends que la maison est couverte par l'alinéa 738(1)*a*), mais la personne pourrait avoir encouru d'autres dépenses en raison du vol de son identité, et la personne a été considérée comme responsable de la situation.

La présidente : Une facture de carte de crédit ne constitue pas un bien.

Le sénateur Joyal : Pour moi, un bien, c'est un immeuble.

M. Nicholson : Monsieur le sénateur, je vais demander à Mme Klineberg de faire un commentaire à cet égard.

Mme Klineberg : Il s'agit d'une question difficile liée à la portée de toutes les conséquences du crime. Les frais directs associés au rétablissement de l'identité seraient couverts. La question à savoir si les frais supplémentaires, comme les frais liés à un procès civil, doivent être couverts constitue un aspect très difficile à aborder en ce qui concerne la mesure dans laquelle on veut recourir au pouvoir de dédommagement dans le droit pénal pour s'occuper de ce qui constitue essentiellement un sujet lié au droit civil. Il existe des inquiétudes en ce qui concerne l'éventuel dédommagement pour beaucoup de choses qui nécessitent l'intervention d'un tribunal civil qui s'engagerait dans un processus d'établissement des faits, afin d'évaluer et de mesurer de façon exacte les coûts engagés, cela serait trop onéreux pour un tribunal criminel dans le contexte d'une audience de détermination de la peine visant à déterminer les coûts. Il est également possible que ces frais ne soient pas connus au moment où la sentence est prononcée à l'encontre d'un contrevenant. S'il y a un genre de procès civil au cours duquel la personne doit, par exemple, s'acquitter d'une fausse hypothèque souscrite sur son bien, cela peut prendre beaucoup de temps avant de déterminer les frais réels se rapportant à l'hypothèque. Il ne serait pas nécessairement facile de déterminer le tout au moment du prononcé de la sentence à l'encontre du contrevenant.

Si vous remarquez dans les alinéas 738(1)*a*), *b*), *c*) et dans le nouvel alinéa proposé d), tous les coûts recouvrables par dédommagement doivent être déjà déterminés. C'est qu'au moment du procès criminel, la cour criminelle doit être en mesure de dire de façon concrète quels sont les coûts afin d'être capable d'ordonner le dédommagement des biens. Lorsqu'on sort de ce contexte, on tombe dans le domaine du droit civil et du dédommagement lié au droit civil.

Senator Joyal: I do not want to prolong the argument, but it seems to me that the line is very thin between being responsible for a mortgage on a property of someone else and losing your own property because your identity has been stolen by someone and your property is sold. It has happened. As you know, we have examples of that.

When it is clear that the damage is there, the mortgage has been registered and you can see the amount because it is there, registered, and it is a real issue in that it is tangible — when the damages are tangible, as that seems to be your preoccupation in terms of concept — I do not see why we could not have a definition that allows for an expansion of the financial responsibility of the author of the fraud.

Ms. Klineberg: I would say only that it would be a question of being able to say that we could be precise about what the nature of those costs would be at the time of the sentencing.

Mr. Nicholson: If it is anything other than that, senator, you know what would happen: The whole matter would be delayed, and you would be getting into another area, which opens the question of civil damages. You and others might say that we are going too far into provincial jurisdiction, that there are civil remedies for lawsuits to proceed and ask why we are getting into this.

This is clean, to the point, precise and easily attainable at the time of sentencing. We do not want to have anything that would delay sentencing.

Senator Joyal: As I say, the damages are tangible, as in the example I have given of a mortgage. It is quite tangible; it is easy to define, to identify. The amount is in the paper.

Mr. Nicholson: Again, senator, this is an improvement over what we have right now. It is a step in the right direction.

Senator Joyal: I am not saying that I am opposed to it.

Mr. Nicholson: I know what you are saying. You are asking why we are not going further. Usually that is not what I get when we introduce legislation. What we have is definable, defensible and a step in the right direction.

Ms. Klineberg: In the case of mortgages, the provincial level has seen increased activity in a variety of provinces. As you mentioned, senator, we have had a number of fraudulent mortgages. In a very high-profile case in Ontario, the Court of Appeal for Ontario actually said that it was the property owner who was responsible for the fraudulent mortgage even though it was the mortgage lender who did all of the paperwork. They subsequently reversed themselves in that particular decision, and provincial governments, as well, have now been legislating in this area in order to allocate any losses in terms of a fraudulent mortgage to the lender and not to the home buyer.

Le sénateur Joyal : Je ne veux pas prolonger la discussion, mais il me semble que la ligne est très mince entre le fait d'être responsable d'une hypothèque prise sur le bien d'une autre personne et le fait de perdre son propre bien parce qu'une autre personne a volé notre identité et a vendu notre bien. Cela est déjà arrivé. Comme vous le savez, nous en avons des exemples.

Lorsqu'il est évident qu'il y a des dommages, que l'hypothèque a été enregistrée et qu'on peut voir le montant car celui-ci a été enregistré et qu'il s'agit d'un véritable problème qui est réel — lorsque les dommages sont réels, comme cela être votre préoccupation en termes de concept — je ne vois pas pourquoi nous ne pourrions pas avoir une définition qui permette une extension de la responsabilité financière de l'auteur de la fraude.

Mme Klineberg : Je dirais seulement qu'il s'agit d'une question d'être en mesure de dire que nous pouvons être précis en ce qui concerne la nature de ces coûts au moment du prononcé de la sentence.

M. Nicholson : S'il y a autre chose, monsieur le sénateur, vous savez ce qui arriverait : toute la question serait retardée, et il faudrait rediriger la question ailleurs, ce qui pose la question des dommages civils. Vous-même et d'autres personnes pourriez dire que nous allons trop loin et que nous empiétons sur la juridiction provinciale, qu'il existe des recours civils pour les poursuites, et vous pourriez demander pourquoi nous abordons ce sujet de cette façon.

C'est clair, direct, précis et facile à réaliser au moment du prononcé de la sentence. Nous voulons que rien ne retarde le prononcé de la sentence.

Le sénateur Joyal : Comme je l'ai dit, les dommages sont réels, comme dans l'exemple que j'ai donné concernant l'hypothèque. C'est très réel; c'est facile à définir et à identifier. Le montant apparaît dans le document.

M. Nicholson : De nouveau, monsieur le sénateur, il s'agit d'une amélioration par rapport à ce que nous avons maintenant. C'est un pas dans la bonne direction.

Le sénateur Joyal : Je ne dis pas que je m'y oppose.

M. Nicholson : Je comprends ce que vous dites. Vous demandez pourquoi nous n'allons pas plus loin. Habituellement, ce n'est pas le résultat que j'obtiens lorsque nous présentons une loi. Ce que nous avons peut être définissable et défendable, et cela constitue un pas dans la bonne direction.

Mme Klineberg : Dans le cas des hypothèques, on a constaté une hausse des activités dans certaines provinces. Comme vous l'avez mentionné, monsieur le sénateur, nous avons un certain nombre d'hypothèques frauduleuses. Dans une affaire très délicate en Ontario, la Cour d'appel de l'Ontario a déclaré en réalité que le propriétaire du bien était responsable de l'hypothèque frauduleuse, même si c'est le prêteur hypothécaire qui a préparé tous les papiers. La Cour a ensuite renversé sa propre décision dans ce cas en particulier, et les gouvernements provinciaux, également, adoptent maintenant des lois dans ce domaine qui abordent toute perte liée à une hypothèque frauduleuse en rendant responsable le prêteur hypothécaire, et non l'acheteur de la maison.

Just specifically with the case of fraudulent mortgages, activity at the provincial level is resolving these issues to the benefit of the property owner.

Senator Angus: Welcome, minister and Ms. Klineberg. Thank you for coming and for your initiative in bringing this law forward. In the last 10 years here, if one subject matter has repeatedly come to my attention as a member of the Standing Senate Committee on Banking, Trade and Commerce requiring study and government intervention and legislation, it has been identity theft.

Based on my understanding from your evidence, this is a first step — or a further step of many — but directed, as you say, more at the macro or organized crime aspects of it where there appears to be evidence of an international clearinghouse. That is what I would like to pursue a bit, if I may.

In Montreal, which I gather is one of the worst centres for this theft, we see cars, especially late model cars, broken into willy-nilly at night. Anything related to identity is taken. There seems to be a very precise modus operandi. They are looking either for computers or wallets with people's gas cards and so on.

Unfortunately, this has happened to me twice in the last year, and the police said basically what you said, that this is organized crime and that I will never see my stuff again. I have lost passports and similar things that were in a suitcase. One does not think of it. Of course, it is easy in hindsight: You should never leave anything in the car.

However, my question to the police and to you, sir, is with respect to what you know and what is driving this legislation. Where do these items go from there? When they are gone, either across our border to the U.S. or over to Milan — I do not know where it goes — nothing happens. I have been waiting with great trepidation. Do they wait for five years and suddenly say, "Okay, now we have had Senator Baker's or Senator Angus' stuff. They were being very vigilant in the wake of the theft, but now it is time."

What happens? Do you have a sense of that?

Mr. Nicholson: I have had a number of discussions, as you can imagine, with law enforcement agencies and people who are trying to deal with this. With your example, someone who kicks in the window of your car and steals your property —

Senator Angus: Identity items.

Mr. Nicholson: Yes, identity items. It is a crime in this country. There is no question about it. The person who steals your credit card or makes a false credit card is a criminal.

It is continuously brought to our attention that this is a larger scheme and that we are not getting everyone. It is similar to auto theft; the laws are out of date, and you will have auto theft before

En ce qui concerne précisément les cas d'hypothèques frauduleuses, les provinces règlent ce genre de cas à l'avantage du propriétaire du bien.

Le sénateur Angus : Bienvenue, monsieur le ministre et madame Klineberg. Merci d'être venus et merci de votre initiative visant à présenter cette loi. Au cours des dix dernières années, si un sujet a été porté à mon attention de façon répétée en tant que membre du Comité permanent des banques et du commerce qui nécessitait une étude et une intervention et une législation du gouvernement, c'est bien le vol d'identité.

Selon ce que je comprends de la preuve que vous avez présentée, il s'agit d'une première étape — ou d'une autre étape parmi de nombreuses autres — mais d'une étape dirigée, comme vous le dites, davantage au niveau macro ou concernant des aspects du crime organisé où il semble exister une preuve de l'existence d'un établissement central à l'échelle internationale. C'est sur cela que j'aimerais poursuivre un peu la discussion, si je le peux.

À Montréal, qui constitue à mon avis un des pires centres pour ce type de vols, nous constatons que des voitures, surtout des modèles récents, qui sont mis en pièces la nuit comme si de rien n'était. Tout ce qui touche à l'identité est visé. Il semble y avoir un modus operandi très précis. Les voleurs cherchent des ordinateurs ou des portefeuilles contenant des cartes d'essence, et cetera.

Malheureusement, cela m'est arrivé deux fois au cours de la dernière année, et la police a déclaré essentiellement la même chose que vous, à savoir qu'il s'agit du crime organisé et que je ne reverrai plus jamais mes biens. J'ai perdu des passeports et des documents de même nature qui se trouvaient dans une valise. On ne pense pas à ça. Bien sûr, c'est facile de le dire *a posteriori* : on ne doit jamais laisser quoi que ce soit dans une voiture.

Mais ce que j'aimerais avoir de la police et de votre part, monsieur, c'est plus d'information sur ce que vous savez et ce qui est derrière cette loi. Où vont nos affaires après? Une fois qu'elles sont rendues de l'autre côté de la frontière, aux États-Unis ou à Milan, ou je ne sais trop où, rien ne se passe. J'attends et je m'inquiète. Est-ce que ces gens laissent passer cinq ans puis se disent : » Bon, nous avons les papiers du sénateur Baker ou du sénateur Angus. Ils devaient être vigilants juste après le vol, mais plus maintenant. »

Qu'est-ce qui arrive? En avez-vous une idée?

M. Nicholson : Comme vous pouvez l'imaginer, j'ai déjà eu des discussions avec des organismes d'application de la loi et des gens qui sont aux prises avec cette question. Vous avez donné l'exemple de quelqu'un qui brise la fenêtre de votre voiture et qui vous vole des biens...

Le sénateur Angus : Des documents d'identité.

M. Nicholson : Oui, des documents d'identité. C'est un crime au Canada, c'est clair. La personne qui vole votre carte de crédit ou qui fabrique une fausse carte de crédit est un criminel.

On nous rappelle tout le temps que ce réseau est vaste et qu'on n'attrape pas tout le monde. On peut faire un rapprochement avec le vol de voiture. Les lois sont désuètes, et un jour vous devrez

you at some point. People tell me the same thing: "Oh, there is a provision in the Criminal Code if you are in possession of the stolen property."

What about the guy who was over here? What about the guy who was marketing this? Many people involved are not captured, and this is what they are telling me about this. When I was in Montreal a year ago with this, a reporter asked me if this was my attempt to get ahead of the bad guys, and I replied that I just want to catch up with the bad guys. This is what we are dealing with; it is ongoing.

Senator Angus: The whole chain of it.

Mr. Nicholson: It is the whole chain.

This is why the proposed legislation is targeted to catch everyone who is in that business. This is what we have to do because these are sophisticated operations. It is not tolerable to only get the person who is actually using the credit card, or the person who actually stole it out of your wallet or out of your car. You have to catch everyone who is part of assembling this for illegal purposes. That is what this proposed law does, and this is why it will be welcomed.

As Senator Wallace indicated, all those individuals who wanted to be there at the press conference who are intimately involved with this whole question are saying that we should update the Criminal Code of this country. This is the challenge we always have with the Criminal Code. People comment that it was written in 1992. However, it was just assembled in 1992. Some of those provisions were 100 years old back then.

We must constantly be looking at these to try to ensure that the sophisticated criminal element out there today is not getting ahead of us.

Senator Angus: You talked about the Internet. We are now dealing in that world of cyberspace.

Mr. Nicholson: It is not confined anymore. It is similar to child pornography. If you go back 50 years, someone produced the child pornography and then sold it. No money is being transferred anymore. Many times, these things are no longer produced in Canada. We have to continuously be looking at the laws to ensure we are capturing the type of illicit activity that is happening out there.

Senator Angus: We are all wrestling with this issue. The car window gets kicked in, stuff happens and the police say to me: "Well, good-bye, Charlie. We have 96 of these a night on average in Montreal between University Avenue and Peel Street, for example. We will never find it. You can look in all the garbage pails yourself, but you will not see it again."

Therefore, I am asking you how this will help.

Mr. Nicholson: It gives them the tools to ensure that anyone who becomes involved in transporting your information, collecting it, shipping it overseas; anyone who is part of the criminal organization will now be covered by this particular

vous pencher sur ce type de crime. Les gens me disent la même chose : » Oh, il existe une disposition dans le Code criminel pour ceux qui sont en possession d'un bien volé. »

Et l'autre gars qui était là? Le gars qui s'occupait de la vente? Bien des personnes impliquées ne sont pas arrêtées, et c'est ce qu'on me dit par rapport à ce problème. Quand j'ai parlé de ce dossier il y a un an à Montréal, un journaliste m'a demandé si j'essayais de garder une longueur d'avance sur les malfaiteurs. Je lui ai répondu que nous voulions seulement les rattraper. Ce que nous faisons, c'est pour faire face à une situation continue.

Le sénateur Angus : Vous parlez de l'ensemble de la chaîne.

M. Nicholson : Oui, de toute la chaîne.

C'est pourquoi le projet de loi cible tous ceux qui jouent un rôle dans ces activités. C'est ce que nous devons faire, parce que ces opérations sont complexes. Ce n'est pas acceptable de se limiter à arrêter seulement la personne qui utilise la carte de crédit, ou la personne qui l'a volée dans votre portefeuille ou votre voiture. Il faut trouver tous ceux qui jouent un rôle dans ces activités illégales. C'est ce que permet ce projet de loi, et c'est pourquoi il sera bien accueilli.

Comme le sénateur Wallace l'a dit, tous ceux qui voulaient être à la conférence de presse, qui s'intéressent de près à l'ensemble de cette question, estiment que nous devons mettre à jour le Code criminel du Canada. Nous avons toujours le même problème avec le Code criminel. Les gens disent qu'il a été rédigé en 1992. Mais il a seulement été assemblé en 1992. Certaines dispositions existaient déjà depuis 100 ans à ce moment.

Nous devons continuellement examiner les dispositions du code pour ne pas être dépassés par des activités criminelles qui, aujourd'hui, sont assez développées.

Le sénateur Angus : Vous avez parlé d'Internet. Il se passe des choses dans le cyberespace.

M. Nicholson : Ce n'est plus un milieu restreint. On peut faire une comparaison avec la pornographie juvénile. Il y a 50 ans, quelqu'un produisait de la pornographie juvénile et la vendait. Mais il n'y a plus de transfert d'argent. Et souvent, ce n'est plus produit au Canada. Nous devons continuellement revoir nos lois pour pouvoir cibler les activités illicites qui ont cours.

Le sénateur Angus : Ce problème nous touche tous. Quelqu'un brise la fenêtre de la voiture, ou quelque chose du genre, et la police me dit : » Eh bien, c'est la vie. Il y a 96 vols de ce genre par soir en moyenne à Montréal, entre l'avenue Université et la rue Peel, par exemple. Nous ne retrouverons jamais vos choses. Vous pouvez chercher dans les ordures vous-même, mais vous n'en reverrez pas la couleur. »

J'aimerais donc que vous nous disiez quelle sera l'utilité de ce projet de loi sur ce plan.

M. Nicholson : Il leur donnera des outils pour cibler toute personne qui joue un rôle dans le processus, qui prend ou transporte vos pièces d'identité, et les envoie outre-mer; la loi vise toute personne qui fait partie de l'organisation criminelle. C'est

legislation. That is exactly what we need to have in this country. We need to have auto theft and child pornography covered — right across the board.

When this type of activity comes to our attention, we have to update the Criminal Code to ensure all of this is captured. This is what this bill does.

[*Translation*]

Senator Nolin: Thank you, Madam Chair. We will now switch to the language of Molière since it is Canada's second official language.

Thank you, Minister, for making the trip to meet with us today.

Senator Joyal: It is one of the two official languages, not the second.

Senator Nolin: Thank you, Senator Joyal.

Minister, I would like to discuss clauses 7 and 9 of the bill, which set out exemptions for government employees, public servants, who make false documents for the federal or provincial governments.

Just under 10 years ago, Parliament enacted section 25.1 of the Criminal Code. My first question is this: Will the procedure set out in section 25.1 apply to the exemptions that you are introducing in clauses 7 and 9 of Bill S-4?

[*English*]

Mr. Nicholson: Senator, are you asking me if there are exceptions? There are exceptions for people who, in good faith, produce documentation, even false documents, if it is pursuant to a legitimate reason.

Senator Nolin: Minister, you are introducing two exceptions. I think those two exceptions are valid; I am not questioning the validity of them. I know the experts have criticized those amendments that were introduced to the Criminal Code in 2001, if my recollection is good. That was section 25.1. Here in the Senate, we introduced some amendments to that bill at that time to ensure the process that was introduced in the code would be respectful of the rule of law and a series of principles.

I want to know if those two exceptions that you are introducing through Bill S-4 will be included in the process introduced in section 25.1. You are repeating in the bill what is already in the code. That is why I want to know why it is you are repeating it. Do you want to exclude those exceptions from section 25.1?

Ms. Klineberg: There are sort of two ways to come at this question.

Senator Nolin: That is exactly why I am asking the question.

exactement ce qu'il nous faut au Canada. Il faut des dispositions pour sévir contre le vol de voitures et la pornographie infantile, en ciblant tous ceux qui sont impliqués.

Quand nous savons que ce type d'activité existe, nous devons mettre à jour le Code criminel pour inclure tous ces aspects. C'est ce que permet ce projet de loi.

[*Français*]

Le sénateur Nolin : Merci, madame la présidente. Nous utiliserons un peu la langue de Molière puisqu'il s'agit de la deuxième langue officielle du Canada.

Merci, monsieur le ministre, de vous être déplacé pour nous rencontrer.

Le sénateur Joyal : Ce n'est pas la deuxième langue, c'est une des deux langues officielles.

Le sénateur Nolin : Merci, sénateur Joyal.

Monsieur le ministre, je voudrais explorer avec vous les articles 7 et 9 du projet de loi qui prévoient des exemptions pour les agents de l'État, les fonctionnaires publics, qui fabriquent des faux documents pour les gouvernements provinciaux et fédéral.

Nous avons adopté au Parlement il y a un peu moins de 10 ans, l'article 25.1 du Code criminel. Ma première question vise à savoir si la procédure prévue à l'article 25.1 s'appliquera aux exemptions que vous introduisez au projet de loi S-4 aux paragraphes 7 et 9 ?

[*Traduction*]

M. Nicholson : Est-ce que vous me demandez s'il y a des exceptions? On a prévu des exceptions pour les gens qui, de bonne foi, fabriquent des documents, même de faux documents, pour une raison légitime.

Le sénateur Nolin : Vous avez prévu deux exceptions, monsieur le ministre. Je crois que ces deux exceptions sont valables. Je ne remets pas leur bien-fondé en question. Je crois que des spécialistes ont critiqué les modifications qui ont été apportées au Code criminel en 2001, si je me souviens bien. Il s'agissait de l'article 25.1. Au Sénat, nous avons fait des amendements à ce projet de loi à l'époque pour nous assurer que le processus qui était inclus dans le code respecterait la règle de droit et certains principes.

J'aimerais savoir si les deux exceptions que vous proposez dans le projet de loi S-4 feront partie du processus prévu à l'article 25.1. Dans le projet de loi, vous répétez ce qui figure déjà dans le code. J'aimerais savoir pourquoi vous le répétez. Voulez-vous exclure ces exceptions de l'article 25.1?

Mme Klineberg : Je dirais qu'il y a deux façons d'aborder cette question.

Le sénateur Nolin : Et c'est pourquoi je pose la question.

Ms. Klineberg: First, in the consultations we held with law enforcement, even independent of this particular piece of legislation, they were especially concerned that the making, the carrying and the using of false identity documents to maintain their covert identities in undercover operations were not easily justified by virtue of section 25.1.

Section 25.1, on their understanding of it, contains a requirement that there already be an investigation under way. In other words, section 25.1 was created to justify, in advance, violations of the criminal law by law enforcement in the course of an investigation that was already underway. Law enforcement told us that they routinely develop and create false covert identities long in advance of there being a particular investigation.

Senator Nolin: I was anticipating that answer. To be honest with you, I was afraid I would hear that answer.

When we introduced section 25.1 in 2001, we had a long discussion about the police doing something illegal. We said that we would agree to that, even though the jurisprudence and the Supreme Court had accepted the principle, but decided to enshrine it in a series of checks and balances, which is fine. The government of the day decided to amend the code. Then the Senate decided to say, "Let us go the full nine yards and really bring Parliament into the loop and ask for a report by the various authorities to tell us, not the detail of the covert operations, but how the rights of Canadians are protected by the police having those extraordinary rights."

When I read the bill and saw those two exceptions, I was afraid I would hear what I just heard. It is tough. We decided to go around the obstacle because the police were asking for that. That is exactly why section 25.1 is there. We do not want to go to the Supreme Court and say that we have a series of excuses, and it was for benefit of law enforcement. That was pleaded before the Supreme Court, and the court decided to enshrine that in a more scrupulous structure.

Ms. Klineberg: May I try the second angle?

Senator Nolin: Of course. That is why we have sober second thought.

Ms. Klineberg: One thing to bear in mind from the outset is that the offence of forgery actually contains a fairly low *mens rea* threshold. The mental state required for making a forged document and using a forged document is simply the intent to deceive. It does not actually require the intent to defraud. For instance, if I wanted to pretend that I have graduated from Harvard Law School and make a phoney certificate on my computer and put that on my wall, maybe with the intention of deceiving someone who walks into my office, that technically speaking might be the offence of forgery, so it is a fairly low threshold.

We understand from law enforcement they may violate that every day when they are acting in an undercover capacity because every day they are acting in an undercover capacity they might be

Mme Klineberg : D'abord, d'après les consultations que nous avons faites avec les organismes d'application de la loi, même en dehors du contexte de ce projet de loi, ils se préoccupaient tout particulièrement du fait que l'article 25.1 ne permettait pas facilement de justifier qu'on fabrique, qu'on transporte et qu'on utilise de fausses pièces d'identité dans les opérations d'infiltration, pour préserver une identité cachée.

D'après leur compréhension de l'article 25.1, il faut qu'une enquête soit déjà en cours. Autrement dit, on a créé l'article 25.1 pour justifier à l'avance une infraction à la législation pénale dans le cadre d'une enquête déjà en cours. Ces organismes nous ont dit qu'il leur arrive souvent d'établir une entité cachée ou une fausse identité bien avant qu'une enquête soit entreprise.

Le sénateur Nolin : Je m'attendais à cette réponse. Pour tout vous dire, je craignais cette réponse.

Lorsque l'article 25.1 a été présenté en 2001, nous avons longuement discuté du fait que la police commette des actes qui seraient illégaux. Nous avons dit que nous serions d'accord, même si la jurisprudence et la Cour suprême avaient accepté ce principe, mais avec un système de contrôle, ce qui est bien. Le gouvernement de l'époque a décidé de modifier le code. Et puis le Sénat a dit : « Allons vraiment jusqu'au bout, faisons intervenir le Parlement, et demandons aux différentes autorités de nous dire, sans nous donner les détails des opérations secrètes, comment les droits des Canadiens sont protégés lorsque la police exerce ces droits extraordinaires. »

Lorsque j'ai vu le projet de loi et que j'ai vu ces deux exceptions, je craignais d'entendre ce que vous venez de me dire. C'est difficile. Nous avons décidé de contourner l'obstacle parce que la police le demandait. C'est exactement pour cette raison que l'article 25.1 existe. Nous ne voulons pas avoir à nous adresser à la Cour suprême et dire que nous avons des excuses, que c'était dans l'intérêt de l'application de la loi. C'est ce qui a été invoqué devant la Cour suprême, et la cour a décidé d'intégrer cet aspect dans une structure plus rigoureuse.

Mme Klineberg : Puis-je essayer sous l'autre angle?

Le sénateur Nolin : Bien sûr. C'est pour cette raison que nous faisons un second examen objectif.

Mme Klineberg : Une chose dont on doit tenir compte dès le départ, c'est que dans le cas du crime de faux et usage de faux, le seuil fixé pour l'intention coupable n'est pas élevé. Pour fabriquer et utiliser un faux document, il suffit d'avoir l'intention de tromper quelqu'un. Il n'est pas nécessaire d'avoir l'intention de frauder. Par exemple, si je voulais prétendre que j'étais diplômée de l'École de droit de Harvard et que je créais un faux certificat sur mon ordinateur pour ensuite l'accrocher au mur, peut-être voulais-je tromper les personnes qui entrent dans mon bureau, et d'un point de vue technique, je pourrais être coupable d'avoir créé un faux document. Le seuil est assez bas.

Nous comprenons que la police peut violer ces dispositions tous les jours lorsqu'ils font des opérations d'infiltration parce que chaque fois, ils risquent d'utiliser une carte de crédit ou une

using a credit card or a business card in the name of their covert identity. It is repetitious. It is many acts of a fairly trivial nature, so it was thought we could justify separate exemptions for this.

Some other offences in the Criminal Code also have exemptions, and child pornography is one of them. Explicit exemptions exist for the possession of child pornography for a purpose related to the administration of justice. Some offences technically are a violation of the law for some people to do, but law enforcement will be in possession of contraband when they receive it, when they confiscate it and when they forfeit it during a criminal investigation. This is just a simple way of saying that they are actually doing their jobs in relation to this small slice of offences, not offences involving bodily harm or involving defrauding anyone, but merely possession of certain types of documents. We thought it was justified in this particular case.

Senator Nolin: I hope the court will agree with that. However, my concern was exactly that because in section 25.1 there is the civilian oversight, the checks and balances and the minister's report just to ensure that someone else is looking after the person who is trying to do his job in good faith but sometimes may, well, cut corners a little bit for the benefit of law enforcement. I hope the court will support and uphold Bill S-4.

Senator Merchant: Minister, thank you for giving us your time to hear our concerns. I have a three-part question, and maybe I will ask all three parts at once.

You spoke of the international dimension of the identity theft. First, have you been engaged with other countries? Are we cooperating with some countries and sharing information with certain countries now?

Second, on a national scope, are you contemplating creating a database as we have for other organized crime in Canada?

Third, I am interested in what we can do to educate the public to understand how to protect themselves against identity theft. We have had one example about people breaking into cars, so we know we should not leave anything in our cars. We frequently see things about how to protect yourself when you go to withdraw money from the bank. Are there things that we should be doing to educate people to try to protect themselves?

Mr. Nicholson: Thank you for those questions, senator.

We share our concerns with other countries, and we have greater cooperation than we have ever had in the past. I give the example of the question of pedophiles. You will notice now that when they are looking for these individuals, these pictures go around the world. This is fairly recent. It is a new innovation to try to track down these individuals so that they have no place to hide. Yes, there is greater cooperation around police forces. Again, it is not specifically related to the justice portfolio, but Interpol and other organizations cooperate with each other to try

carte professionnelle établies au nom de leur couverture. Ils font ces gestes à répétition. Il s'agit de gestes plutôt banals et on a cru que des exemptions distinctes étaient justifiables dans ces cas.

Des exemptions sont également prévues pour d'autres infractions au Code criminel, dont la pornographie juvénile. On retrouve des exemptions claires concernant la possession de pornographie juvénile dans un dessein lié à l'administration de la justice. Certaines personnes violent techniquement la loi en commettant certaines infractions, mais la police peut être en possession de matériel de contrebande lorsqu'elle en reçoit et lorsqu'elle en confisque au cours d'une enquête criminelle. C'est une façon simple de dire qu'ils font leur travail en ce qui concerne cette catégorie limitée d'infractions, qui ne causent pas de lésions corporelles et qui ne constituent pas une fraude. Il s'agit seulement d'être en possession de certains types de documents. Nous croyons que c'était justifié dans ce cas précis.

Le sénateur Nolin : J'espère que la cour en conviendra. Cependant, c'est exactement ce que je craignais. Dans l'article 25.1, on parle de surveillance civile, de contrepoids, et des rapports du ministre uniquement pour s'assurer qu'on surveille les personnes qui tentent de faire leur travail de bonne foi, mais qui doivent parfois tourner les coins ronds pour appliquer la loi. J'espère que la cour appuiera le projet de loi S-4 et confirmera sa validité.

Le sénateur Merchant : Monsieur le ministre, merci de nous accorder du temps pour que nous puissions vous faire part de nos préoccupations. J'ai une question à trois volets, et je pense que je vais les présenter les trois en même temps.

Vous avez parlé de la dimension internationale du vol d'identité. Premièrement, avez-vous pris des mesures avec d'autres pays? Collaborons-nous et échangeons-nous actuellement de l'information avec certains pays?

Deuxièmement, sur le plan national, envisagez-vous de créer une base de données comme nous l'avons fait pour d'autres types de crimes commis par des groupes organisés au Canada?

Troisièmement, je m'intéresse à ce que nous pourrions faire pour sensibiliser le public afin qu'il comprenne comment il doit se protéger contre le vol d'identité. On nous a déjà donné l'exemple d'individus qui entraient par infraction dans des véhicules pour nous faire comprendre que nous ne devons rien laisser dans nos autos. On nous dit souvent comment nous protéger lorsque nous faisons un retrait à la banque. Y a-t-il des choses que nous pouvons faire pour éduquer les gens afin qu'ils prennent des mesures pour se protéger?

M. Nicholson : Je vous remercie pour vos questions, madame.

Nous partageons nos préoccupations avec les autres pays, et la collaboration est meilleure que jamais. Je peux vous parler par exemple des pédophiles. Vous remarquerez maintenant que lorsque nous recherchons ces individus, leurs photos font le tour du monde. C'est assez récent. Nous avons innové pour tenter de retracer ces individus afin qu'ils n'aient nulle part où se cacher. Oui, la collaboration est plus grande entre les forces policières. Encore une fois, ce n'est pas particulièrement lié au portefeuille de la justice, mais Interpol et les autres organismes travaillent de

to track these people down. In terrorism, for instance, we know of the cooperation between our country and Great Britain and the United States and other countries in terms of trying to track down these individuals because we are all exposed to the damage these individuals can cause.

I do not have any specific plans on a database with respect to this legislation, but I thank you for your comments on that.

We are making these announcements and bringing in people from the private sector as part of this education process. Certainly in my conversations with stakeholders, I say the same thing to them that they have to get this message out to their customers and to people. I do think there is a greater awareness today. People understand the pitfalls and the challenges of protecting their own information. Between government, private sector and individuals, the message is getting out there that this is a continuous problem, and it could get worse, which is one of the reasons we are bringing this legislation forward.

Senator Merchant: Specifically, how will you educate people to protect themselves? I am talking about government, not about people talking to their customers.

Mr. Nicholson: I am not announcing any new program. We have announced programs on a national anti-drug strategy. We keep announcing programs. We work with NGOs and community groups. I am not announcing any specific program to launch identity theft awareness. However, again, in my discussions with stakeholders, I tell them that they have a great deal at stake here in ensuring that the message gets out. I have been pleased with their response.

Senator Bryden: Thank you, Minister, for coming.

I will be brief and also get off topic a little and talk about some of the drafting that is in here, or the terminology. The first one that hit me is in proposed new section 56.1(1). I think I understand it, but I am not sure.

> Every person commits an offence who, without lawful excuse, procures to be made, possesses, transfers, sells or offers for sale an identity document that relates or purports to relate, in whole or in part, to another person.

Why is the phrase "procures to be made" there? It is a strange combination of words.

Mr. Nicholson: I will ask the drafter the question.

Ms. Klineberg: In that context, we were thinking that if an individual were to use false information to make an application — for example, a passport or driver's licence — it would be the act of trying to get the document issued, in and of itself, in a false name. That is what we were trying to capture by "procuring" to be made.

Senator Milne: Therefore, it should be "causes" to be made, not "procures" to be made.

concert pour retrouver ces personnes. Il y a aussi le terrorisme. Par exemple, nous savons que le Canada, la Grande-Bretagne, les États-Unis, ainsi que d'autres pays, mettent leurs efforts en commun pour retracer ces individus, parce que nous sommes tous exposés aux torts qu'ils peuvent causer.

En ce qui concerne une base de données qui serait utilisée relativement à cette loi, je n'ai pas de plan précis, mais je vous remercie pour vos commentaires à ce sujet.

Pour le processus d'éducation, nous faisons ces annonces et nous faisons participer des gens du secteur privé. Lorsque je discute avec les intervenants, je leur dis toujours la même chose, c'est-à-dire qu'ils doivent transmettre le message à leurs clients et au grand public. Je crois qu'il y a bel et bien une plus grande sensibilisation aujourd'hui. Les gens comprennent les embûches et les défis que représente la protection de leurs renseignements. Le message qui circule entre le gouvernement, le secteur privé et les particuliers, c'est que nous faisons face à un problème chronique qui peut devenir plus grave. Ça explique en partie pourquoi nous présentons ce projet de loi.

Le sénateur Merchant : Plus particulièrement, comment inciterez-vous les gens à se protéger? Par « vous », je parle du gouvernement, et non de ceux qui parlent à leurs clients.

M. Nicholson : Je n'annonce pas de nouveau programme. Nous avons annoncé des programmes relativement à la stratégie nationale antidrogue. Nous annonçons continuellement des programmes. Nous travaillons avec les ONG et les groupes communautaires. Je n'ai aucun programme particulier de sensibilisation contre le vol d'identité à annoncer. Cependant, lors de mes discussions avec les intervenants, je leur dis qu'ils ont beaucoup en jeu et qu'ils doivent s'assurer que le message est transmis. Et ils réagissent bien.

Le sénateur Bryden : Monsieur le ministre, merci d'être venu.

Je serai bref. Je vais m'écarter un peu du sujet pour parler du libellé ou de la terminologie utilisés. La première chose qui m'a frappé se trouve dans la version anglaise du nouveau paragraphe 56.1(1). Je crois comprendre, mais je ne suis pas certain.

> Every person commits an offence who, without lawful excuse, procures to be made, possesses, transfers, sells or offers for sale an identity document that relates or purports to relate, in whole or in part, to another person.

Pourquoi dit-on « procures to be made »? Cette tournure est étrange.

M. Nicholson : Je poserai la question au rédacteur.

Mme Klineberg : Dans ce contexte, nous nous disions que si un individu devait utiliser de faux renseignements pour faire une demande, par exemple, pour obtenir un passeport ou un permis de conduire, il tenterait par ce geste de faire délivrer le document lui-même sous un faux nom. C'est ce que nous tentions de rendre par « procuring to be made ».

Le sénateur Milne : Par conséquent, ça devrait être « causes to be made », et non « procures to be made ».

Ms. Klineberg: I could not tell you how many times we go around in circles in drafting this. I could not say that we have necessarily got all the words in the only form in which they could have been drafted. However, that is what was intended with that wording.

Senator Bryden: Senator Milne, I think the word "causes" is well understood by most people.

Mr. Nicholson: We will look at that and get back to you.

Senator Bryden: Having done some drafting myself, there is a tendency for some drafters to want to write poetry so as not to repeat the same word over and over. However, you are trying for clarity not poetry in preparing a piece of legislation.

Clause 5 of the bill amends subsection 342.01(1) of the act, which states that:

> (1) Every person is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years, or is guilty of an offence punishable on summary conviction, who, without lawful justification or excuse, makes, repairs, buys, sells . . . .

I understand that and it appears in the bill a couple of times. However, I have a Senator Baker piece here that I could not pass by. Clause 4 of the bill says:

> Every person who, fraudulently and without colour of right, possesses, uses, traffics in or permits another person to use . . . .

Why would you choose to use the terminology, which some might say was archaic, of "colour of right" in this?

Mr. Nicholson: I did not know it was that archaic, senator. I thought that term was rather common.

Ms. Klineberg: Clause 4 pertaining to amendments of subsection 342(3) of the Criminal Code is an offence currently in the Criminal Code. It has that phrase in it. You might see different language in that offence than you would in the offence from clause 5 pertaining to subsection 342.01(1). Clause 5 in the bill deals with the making, possession, import and export of instruments — actual things — whereas clause 4 pertaining to subsection 342(3) deals with misconduct in relation to another person's credit card information. There is an element of fraud, deception and dishonesty involved in the use of another person's information that is not present in relation to the offence for making or repairing instruments for use in crime. That is why you would see something like "fraudulently" used in the one offence and not the other.

Again, these are offences currently in the Criminal Code. It is another of those difficult decisions we face: Should we take the opportunity when amending the legislation for one purpose to make it consistent with other offences in other ways? Oftentimes, we decide not to do that because it creates difficulties for police and prosecutors who would have to prosecute offences worded

Mme Klineberg : Je ne peux pas vous dire à quel point nous avons travaillé la formulation. Je ne peux pas affirmer que nous avons utilisé la seule bonne formule lors de la rédaction. Cependant, c'est ce que nous voulions dire.

Le sénateur Bryden : Monsieur Milne, je crois que le mot « causes » est bien compris par la plupart des gens.

M. Nicholson : Nous examinerons la question et vous donnerons une réponse.

Le sénateur Bryden : J'ai moi-même fait un peu de rédaction. Certaines personnes ont tendance à vouloir faire de la poésie en tentant d'éviter les répétitions. Cependant, lorsqu'on rédige une loi, on vise la clarté; il ne s'agit pas de poésie.

L'article 5 du projet de loi modifie le paragraphe 342.01(1) de la loi, dans lequel on peut lire en anglais :

> (1) Every person is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years, or is guilty of an offence punishable on summary conviction, who, without lawful justification or excuse, makes, repairs, buys, sells [...]

Je comprends ça et on peut le lire dans le projet de loi à deux ou trois reprises. Cependant, il y a un élément du sénateur Baker sur lequel je ne peux pas fermer les yeux. On peut lire à l'article 4, toujours en anglais :

> Every person who, fraudulently and without colour of right, possesses, uses, traffics in or permits another person to use [...]

Pourquoi choisissez-vous d'utiliser cette terminologie, ce « colour of right », qui peut sembler archaïque pour certains?

M. Nicholson : Je ne savais pas que c'était archaïque, monsieur le sénateur. Je croyais que ce terme était plutôt courant.

Mme Klineberg : L'article 4, qui porte sur les modifications au paragraphe 342(3) du Code criminel, traite d'une infraction qui se trouve déjà dans le code. Cette expression s'y trouve. Le libellé y est différent de celui de l'article 5, qui concerne le paragraphe 342.01(1). L'article 5 traite de la fabrication, de la possession, de l'importation et de l'exportation d'instruments — des choses concrètes — tandis que l'article 4, qui modifie le paragraphe 342(3), traite de l'inconduite relative à l'information qui se trouve sur la carte de crédit d'une autre personne. L'élément de fraude, de tromperie et de malhonnêteté qu'on trouve dans l'utilisation des renseignements d'autrui ne se trouve pas dans les cas de la fabrication ou de la réparation d'instruments utilisés pour le crime. C'est pourquoi on voit un terme comme « frauduleusement » être utilisé pour une infraction et pas pour l'autre.

Je voudrais rappeler que ces infractions se trouvent actuellement dans le Code criminel. C'est une autre décision difficile que nous avons dû prendre. Devons-nous profiter de l'occasion lorsque nous modifions la loi pour assurer une certaine uniformité avec les autres infractions? Souvent, on décide de ne pas le faire parce que cela crée des difficultés pour la police et

slightly different. We sometimes decide simply to maintain the wording where there does not appear to be a problem with interpretation or application of the offences.

The Chair: While on the subject of prose, I understand how it came to be, but I draw your attention to proposed new section 56.1(3):

> For the purposes of this section, "identity document" means a Social Insurance Number card, a driver's licence, a health insurance card, a birth certificate, a passport as defined in subsection 57(5), a document that simplifies the process of entry into Canada, a certificate of citizenship, a document indicating immigration status in Canada or a certificate of Indian status, issued or purported to be issued by a department or agency of the federal government or of a provincial government, or any similar document issued or purported to be issued by a foreign government.

I read that three times before I was sort of satisfied that all of the documents it refers to had to be issued or were purported to be issued by a department or agency of a government. I wonder if it might not be possible to reword it slightly to make it clearer from the outset. I know that the entire section is headed "Official Documents." However, that particular paragraph strikes me as virtually indigestible and unusually the French was not much help. Often the French is clearer than the English, but I did not find it to be so in this case.

Mr. Nicholson: Do you suggest we come up with a better definition of government documents?

The Chair: No, simply make it clearer that every single document listed, and not only the last one in that list, is to be a document issued by a government. You have a series of commas and after one of the commas you have "issued or purported to be issued by a department or agency of the federal government." As I say, I found it quite indigestible. Maybe every lawyer in the land finds it crystal clear. I did not.

Senator Nolin: No, it is worse.

Mr. Nicholson: I thought lawyers liked definitions like that.

The Chair: They are very lucrative.

I have been informed that minister has a vote in 10 minutes. Minister, we did have more questions. Could I ask Senator Baker and Senator Joyal to pose their questions? Maybe you could write back to us or perhaps Ms. Klineberg could remain and answer them if they are within her purview. I am sorry, honourable senators; I did not know this was the case.

Senator Baker: My question relates to Senator Joyal's line of questioning. As you indicated, the civil remedy is brought into the Criminal Code for compensation purposes that result from the

pour les procureurs, qui dans leurs poursuites devraient utiliser des énoncés un peu différents. Nous décidons parfois de simplement utiliser les mêmes mots lorsqu'il ne nous semble pas y avoir de problème avec l'interprétation de ces infractions ou à l'étape de l'application.

La présidente : Tandis que nous sommes dans le sujet de la rédaction, je comprends comment cela s'est trouvé ici, mais j'aimerais attirer votre attention sur le libellé anglais du paragraphe 56.1(3), que je vais lire :

> For the purposes of this section, "identity document" means a Social Insurance Number card, a driver's licence, a health insurance card, a birth certificate, a passport as defined in subsection 57(5), a document that simplifies the process of entry into Canada, a certificate of citizenship, a document indicating immigration status in Canada or a certificate of Indian status, issued or purported to be issued by a department or agency of the federal government or of a provincial government, or any similar document issued or purported to be issued by a foreign government.

J'ai dû lire cet énoncé trois fois avant de comprendre que tous les documents auxquels on se réfère doivent être délivrés ou paraître être délivrés par un ministère ou un organisme d'un gouvernement. Je me demandais s'il serait possible de reformuler un peu afin que l'on comprenne dès le départ. Je sais que l'article au complet est intitulé « Documents officiels ». Cependant, ce paragraphe en particulier est à mes yeux presque illisible et, fait rare, le français n'a pas beaucoup aidé. Souvent le français est plus clair que l'anglais, mais je ne trouvais pas que c'était le cas ici.

M. Nicholson : Est-ce que vous suggérez que nous définissions mieux quels sont les documents du gouvernement?

La présidente : Non, j'aimerais simplement qu'il soit clairement établi que tous les documents de la liste, et non seulement le dernier, sont des documents délivrés par le gouvernement. Il y a une série de virgules et après l'une d'elles, on trouve « issued or purported to be issued by a department or agency of the federal government ». Comme je disais, je trouvais ça très lourd. Peut-être que tous les avocats du pays trouvent que c'est clair. Ce n'était pas mon cas.

Le sénateur Nolin : Non, c'est pire.

M. Nicholson : Je croyais que les avocats aimaient ce genre de définitions.

La présidente : C'est très lucratif.

On m'a informé que le ministre a un vote dans 10 minutes. Monsieur le ministre, nous avions d'autres questions. Est-ce que je pourrais inviter les sénateurs Baker et Joyal à poser leurs questions? Peut-être pourriez-vous nous donner une réponse par écrit, ou peut-être Mme Klineberg pourrait-elle rester avec nous et répondre à ces questions si elles font partie de son mandat. Je suis désolée, chers collègues; je n'étais pas au courant.

Le sénateur Baker : Ma question se rapporte aux questions du sénateur Joyal. Comme vous l'avez indiqué, le recours civil est intégré au Code criminel à des fins d'indemnisation à la suite d'un

commission of a crime. Am I to understand that this will be a procedure similar to that of forfeiture under the Criminal Code? In other words, it will be a procedure after sentencing, after someone is found guilty. Then there will be a judgment by the court as recommended by the Crown as to the extent of the damage. In other words, will it mirror a forfeiture judgment after sentencing?

Senator Joyal: When Bill C-27 was introduced, the Privacy Commissioner raised the issue that the bill as drafted at that time did not cover the spam or phishing initiative, a common crime to induce people to believe that you are a person in authority to phish information. We know there are many "victims" of that initiative. Is it correct that that preoccupation expressed by the Privacy Commissioner is not covered by Bill S-4 as drafted now?

Mr. Nicholson: I will leave Ms. Klineberg with you. I will confer with her on the answers to that, and we will get back to you on any other information you may need.

The Chair: We thank you, and I apologize. Votes matter, and I did not realize you had one coming.

Do you have answers to those questions, Ms. Klineberg, before we continue?

Ms. Klineberg: With respect to the second question, Senator Joyal's question, I was just informed as the minister's staff was leaving that the Minister of Industry has just tabled a spam bill.

Senator Joyal: Will it be covered individually?

Ms. Klineberg: Unfortunately, I am not in a position to say much more on it.

Senator Angus: Yes, I think that was intention.

Ms. Klineberg: I think it is a comprehensive legislation.

The Chair: I am informed that that is Bill C-27. We can inform ourselves about it as we proceed.

Ms. Klineberg: With respect to phishing, to the extent that a phishing attack is designed to elicit from people their own personal information, it could constitute an attempted identity theft, so it is not explicitly dealt with in the bill. However, phishing is a method of committing identity theft; it is one of the many methods of doing that. A phishing attack, if that is its purpose, could be an offence of attempted identity theft. If it is successful and people do respond by providing their information, that would be an identity theft.

Senator Joyal: Should we not spell out the attempt clearly in the bill?

crime qui a été commis. Dois-je comprendre qu'il s'agira d'une procédure similaire à celle de la confiscation en vertu du Code criminel? Autrement dit, il s'agira d'une procédure après détermination de la peine, après que la personne aura été déclarée coupable. Ensuite, le tribunal rendra un jugement fondé sur la recommandation de la Couronne en ce qui concerne l'étendue des dommages-intérêts. Autrement dit, la procédure ressemblera-t-elle à un jugement de confiscation après détermination de la peine?

Le sénateur Joyal : Lorsque le projet de loi C-27 a été présenté, la commissaire à la protection de la vie privée a souligné que le projet de loi tel que rédigé à l'époque ne s'appliquait pas au pourriel ou à l'hameçonnage, un crime répandu qui vise à amener les gens à croire qu'on est une personne autorisée à leur soutirer de l'information. Nous savons que cette initiative fait beaucoup de « victimes ». Est-ce une bonne chose que la préoccupation exprimée par la commissaire à la protection de la vie privée ne figure pas dans le projet de loi S-4 tel que rédigé actuellement?

M. Nicholson : Je vous laisse avec Mme Klineberg. Je m'entretiendrai avec elle à propos des réponses à ces questions, et nous communiquerons avec vous pour vous donner d'autres renseignements dont vous pourriez avoir besoin.

La présidente : Nous vous remercions, et je m'excuse. Les votes comptent, et je ne savais pas que vous en aviez un sous peu.

Avez-vous des réponses à ces questions, madame Klineberg, avant de poursuivre?

Mme Klineberg : En ce qui concerne la seconde question, la question du sénateur Joyal, en quittant, le personnel du ministre m'a informée que le ministre de l'Industrie venait de déposer un projet de loi sur le pourriel.

Le sénateur Joyal : Le pourriel sera-t-il examiné individuellement?

Mme Klineberg : Malheureusement, je ne peux pas en dire plus à ce sujet.

Le sénateur Angus : Oui, je crois que c'est ce qui est prévu.

Mme Klineberg : Je crois qu'il s'agit d'une loi exhaustive.

La présidente : On m'informe qu'il s'agit du projet de loi C-27. Nous pouvons nous informer à ce propos à mesure que nous avançons.

Mme Klineberg : En ce qui concerne l'hameçonnage, dans la mesure où l'hameçonnage vise à tenter d'obtenir les renseignements personnels des gens, cela constituerait une tentative de vol d'identité, alors le projet de loi n'en parle pas explicitement. Toutefois, l'hameçonnage est une façon de commettre un vol d'identité; c'est l'une des nombreuses façons de le faire. L'hameçonnage, si c'est là le but qu'il vise, pourrait constituer une infraction de tentative de vol d'identité. Si c'est réussi et que les gens répondent en fournissant leurs renseignements, cela constituerait un vol d'identité.

Le sénateur Joyal : Ne devrions-nous pas expliquer clairement la tentative dans le projet de loi?

Ms. Klineberg: I think section 24 in the Criminal Code is the general provision for attempt. Attempting to commit any offence constitutes an attempt, so for most offences, we do not spell out that attempting to do something would constitute an offence. We usually just leave it for the general application of section 24 in the Criminal Code.

Senator Joyal: On clause 11 of the bill, again, on the wording of the examples that are given as expenses that someone might incur to re-establish their identity, I read "including expenses to replace their identity documents." That is easily understandable. If you want to replace your passport, that is easy, or if you want to have another birth certificate or another social insurance number or health insurance card and so on.

More problematic, and I am looking at Senator Angus on this, is the part that says, "and to correct their credit history." What are the expenses to correct the credit history?

This concept is very broad because we can imagine any type of situation. If I have to re-establish my credit history with a bank, a financial institution, a credit card company or any institution that deals with credit, it might mean a lot because the institution might ask for me to pay back expenses that they had to incur to face the responsibility and so forth. This is a very broad concept.

What do we have to understand by re-establishing credit history? What do you include in that?

Ms. Klineberg: With Equifax, for example, I think you can obtain one free copy of your credit rating per year, so if you were to try to obtain many of them to verify that changes you had made were being incorporated into their documents, there would be costs associated with ordering those.

The examples you mentioned might also apply. It was, as you say, meant to be somewhat broad. We did not want to be listing specifically all of the potential things for which people might seek restitution. As you say, we went for the concept instead, so that people or the Crown on behalf of the victim could make arguments that certain costs should be covered.

I can not give you much more in the way of detail to what that could cover, but the idea was direct costs related to the victimization of a person having their identity stolen.

It would be for the Crown to argue exactly how that might play out in any particular case.

Senator Joyal: That is subject to the last sentence, the last words, "if the amount is readily ascertainable.

Ms. Klineberg: Exactly; that always has to be part of an order for restitution because the criminal court is not in a position to engage in the same sort of analysis that a civil court would do to determine remedies. The criminal court needs to have put before it

Mme Klineberg : Je crois que l'article 24 du Code criminel est la disposition générale pour les tentatives. Le fait de tenter de commettre une infraction constitue une tentative, alors pour la plupart des infractions, nous n'expliquons pas clairement que le fait de tenter de faire quelque chose constituerait une infraction. Habituellement, nous le laissons simplement à l'application générale de l'article 24 du Code criminel.

Le sénateur Joyal : À l'article 11 du projet de loi, encore une fois, le libellé des exemples qui sont donnés concernant les dépenses qu'une personne peut engager liées au rétablissement de son identité se lit « notamment pour corriger son dossier ». C'est facile à comprendre. Si on veut remplacer notre passeport, c'est facile, ou si on veut obtenir un autre certificat de naissance, n^{o} d'assurance sociale, carte d'assurance maladie, et cetera.

Ce qui est plus problématique, et je regarde le sénateur Angus à ce propos, c'est la partie qui dit « et sa cote de crédit ». Quelles sont les dépenses liées à la correction d'une cote de crédit?

Ce concept est très large parce que nous pouvons imaginer toutes sortes de situations. Si je dois rétablir ma cote de crédit auprès d'une banque, d'une institution financière, d'une société émettrice de carte de crédit ou d'une autre institution associée au crédit, cela peut signifier beaucoup, car l'institution pourrait me demander de rembourser les dépenses qu'elle a dû engager pour assumer cette responsabilité, et cetera. C'est un concept très large.

Que devons-nous comprendre par rétablissement du dossier de crédit? En quoi cela consiste-t-il?

Mme Klineberg : Avec Equifax, par exemple, je crois qu'on peut obtenir un exemplaire gratuit de notre cote de crédit par année, alors si on essayait d'en obtenir beaucoup d'autres pour s'assurer que les changements qu'on a apportés ont été insérés dans leurs documents, il y aurait des coûts associés à ces exemplaires.

Les exemples que vous avez mentionnés pourraient également s'appliquer. Comme vous le dites, le concept a été rédigé de façon assez large. Nous ne voulions pas énumérer spécifiquement toutes les choses potentielles pour lesquelles les gens pourraient réclamer un dédommagement. Comme vous le dites, nous avons plutôt misé sur le concept afin que les gens ou que la Couronne, au nom de la victime, puissent présenter des arguments qui feraient en sorte que certains coûts seraient remboursés.

Je ne peux pas vous donner beaucoup d'autres détails sur ce qui serait compris, mais l'idée c'était que les coûts directs liés à la victimisation d'une personne qui se serait fait voler son identité seraient remboursés.

Ce serait à la Couronne de présenter des arguments sur la façon exacte dont ça pourrait se passer dans un cas particulier.

Le sénateur Joyal : Cela est assujetti à la dernière phrase, aux derniers mots : « si ces dommages peuvent être facilement déterminés ».

Mme Klineberg : Exactement, cela doit toujours faire partie d'une ordonnance de dédommagement parce que le tribunal pénal ne peut pas entreprendre le même genre d'analyse qu'un tribunal civil pour déterminer les recours. Le procureur doit avoir déposé

on the part of the prosecutor readily ascertainable and relatively clear costs associated with the crime. It will always be subject to that particular qualification, but the nature of the claims might be subject to some broader interpretation.

Senator Baker: My question relates to my earlier question, which was not addressed. The reason I ask the question is precisely the line of questioning that Senator Joyal was following.

Under the present sections of the Criminal Code, when you have forfeiture involved, under various sections, it is readily available because the forfeiture provisions have a value already done, or it is the forfeiture of money to the Crown, a forfeiture of the value of the offence that was committed. It is readily available, so that if someone pleads guilty to an offence and the trial does not go on for a year, two years, three years or four years, as some do, the Crown is able to immediately identify an amount of money.

However, in this case, as Senator Joyal has pointed out, it could have ramifications down the road. That is why in civil actions you usually wait for two to five years to find out the results of the offence for which you are trying to collect compensation.

In this case, it has to be immediate, with some formula in advance. Do you anticipate, have you had any representations or have you turned your mind to the sort of a formula that would be suggested to the Crowns to address that very serious problem? It could be something happening two years in the future.

You could say that we will turn to the civil courts, but you have it now here in legislation. Have you turned your mind to a formula?

Ms. Klineberg: Nothing that I would quite call a formula. I would anticipate that Crown prosecutors would undertake the same sort of analysis they would for other claims that they try to make for restitution under subsections 738(1)(*a*), (*b*) and (*c*) of the Criminal Code. There might be physical injuries, the remedy for which is still ongoing after the time of trial, which would not be covered by a restitution order. It is not meant to replace a civil proceeding. Restitution is designed as part of the sentence to instill a sense of responsibility on the part of the offender. It is not meant to be a road to complete recovery and remedy for the victim.

Senator Baker: If that very question were adjudicated in the criminal court, you are surely not suggesting that someone could then ask for a reajudication of the same question in the civil action following?

Ms. Klineberg: No, it is a different route to a remedy for compensation. There is overlap as well in terms of subsections 738(1)(*a*), (*b*) and (*c*). Those losses as well could be claimed in a civil suit. Alternative methods are available for the victim to obtain some form of restitution.

devant le tribunal pénal les coûts facilement déterminés et relativement clairs associés au crime. Cela sera toujours assujetti à cette qualification particulière, mais la nature des réclamations pourrait faire l'objet d'une interprétation plus large.

Le sénateur Baker : Ma question a trait à la question que j'ai posée plus tôt, à laquelle je n'ai pas obtenu de réponse. Je pose la question parce qu'elle s'inscrit dans la série de questions du sénateur Joyal.

En vertu des articles actuels du Code criminel, lorsqu'il y a confiscation, en vertu de divers articles, c'est facilement disponible, car les dispositions sur la confiscation ont déjà une valeur, ou il s'agit de la confiscation d'argent à la Couronne, une confiscation de la valeur de l'infraction qui a été commise. C'est facilement disponible, de sorte que si une personne plaide coupable à une infraction et que le procès ne se déroule pas avant un an, deux ans, trois ans ou quatre ans, comme c'est le cas pour certains, la Couronne est en mesure de déterminer immédiatement un montant d'argent.

Toutefois, dans le présent cas, comme l'a mentionné le sénateur Joyal, il pourrait y avoir des conséquences plus tard. C'est pourquoi lors des poursuites civiles, on attend habituellement entre deux et cinq ans pour obtenir les résultats de l'infraction pour laquelle on essaie d'obtenir une indemnité.

Dans le présent cas, cela doit être immédiat, au moyen d'une certaine formule établie à l'avance. Avez-vous une idée de la formule qui pourrait être proposée à la Couronne pour régler ce problème très sérieux? Avez-vous reçu des observations à ce chapitre ou avez-vous examiné le type de formule qui pourrait être proposé? Cela pourrait se produire dans deux ans.

Vous pourriez dire que nous nous tournerons vers les tribunaux civils, mais le recours civil figure maintenant dans la loi. Avez-vous examiné une formule?

Mme Klineberg : Rien que j'appellerais une formule. Selon moi, les procureurs de la Couronne entreprendraient le même genre d'analyse que pour d'autres réclamations qu'ils essaient de faire pour obtenir un dédommagement en vertu des alinéas 738(1) *a*), *b*) et *c*) du Code criminel. Il peut s'agir de lésions physiques, dont le recours se poursuivrait toujours après le procès et ne pourrait faire l'objet d'une ordonnance de dédommagement. Il ne vise pas à remplacer une procédure civile. Le dédommagement fait partie de la phrase afin d'instaurer un sens des responsabilités chez le contrevenant. Il n'est pas censé être un chemin vers le recouvrement et le recours complets pour la victime.

Le sénateur Baker : Si cette question devait être jugée par un tribunal criminel, vous ne voulez sûrement pas dire que quelqu'un pourrait demander qu'elle soit jugée de nouveau dans le cadre d'une poursuite civile subséquente?

Mme Klineberg : Non, c'est une voie de recours différente pour le dédommagement. Il y a également chevauchement en ce qui a trait aux paragraphes 738(1)*a*), *b*) et *c*). Ces pertes pourraient être également réclamées dans une poursuite au civil. En fait, la victime peut recourir à d'autres méthodes pour obtenir la restitution de biens.

There is an advantage from a criminal-justice perspective to this being part of the sentence because it, as part of the criminal law, as opposed to a civil law, creates a sense of responsibility and a duty to repair the crime on the part of the offender, which is a slightly different way of approaching the situation civilly. It is an alternative route to the same sorts of things, but it is much more limited, and, therefore, the amounts have to be readily ascertainable much more quickly. It is also easier for the victim who would not have to go through the process of suing if the restitution they could get criminally were sufficient for them.

Senator Joyal: Once you are found guilty, compensation as provided in clause 11 is almost automatic.

If you go to civil litigation, it is a totally different type of action, and you might not get as much as you get on this one, especially in terms of re-establishing. Look at what it means: credit history and credit rating. In some circumstances, it could be quite something, especially if you think about those organized groups that are "well oiled" in trying to extort money through all sorts of devices.

It is a very important concept we are introducing in there. Senator Nolin knows the issue of claims or damages in civil litigation. It is a whole set of different kind of approaches in the Criminal Code that we have in there. Those are intangible damages, while section 738(1) is property. Property is hard, whereas a credit rating or history is intangible.

Senator Angus: No, she was talking about direct costs involved in re-establishing the intangible. It is different.

Senator Joyal: It is much different. That is why I draw the attention of the minister, you and honourable senators to this. I am not opposed to it in principle, but how do we evaluate it? How do we frame it? What are its side consequences?

In my opinion, those are very important issues. We might want to hear about this from other witnesses because I feel it is an important element of this bill.

Senator Angus: If I understand it, this is an additional penalty. You have fairly strong penalties of imprisonment and so on. This restitution is an additional sanction of some kind and, therefore, I imagine, designed to be a deterrent. That is what these penalties are all about; to make them such that the criminals are deterred and encouraged not to commit the crime.

I think you are saying that it is not that clear and these direct costs are probably *de minimis* in most cases. If Equifax charges $50, the costs involved really with Equifax and the

Du point de vue de la justice criminelle, il y a un avantage à intégrer cet élément dans la peine imposée parce que, dans le contexte du droit criminel, par opposition au droit civil, cela crée un sentiment de responsabilité et une obligation de réparation de la part du contrevenant, ce qui constitue une approche légèrement différente par rapport à la situation d'un point de vue civil. Il s'agit d'un recours différent pour ce genre de choses, mais il est beaucoup plus limité et, par conséquent, les montants doivent être garantis plus rapidement. C'est également un recours plus facile pour une victime qui ne souhaite pas entamer de poursuites lorsqu'elle estime suffisant le dédommagement qu'elle peut obtenir.

Le sénateur Joyal : Ainsi, une fois que vous êtes trouvé coupable, le dédommagement prévu à l'article 11 s'applique presque automatiquement.

Par ailleurs, si la victime s'adresse à un tribunal civil, c'est un type de mesure tout à fait différent et cette personne pourrait ne pas obtenir autant que par ce recours, plus particulièrement du point de vue du dédommagement. Il faut voir ce que cela signifie au niveau des antécédents en matière de crédit et de la cote de crédit. Dans certaines situations, cela peut signifier beaucoup, plus particulièrement si vous pensez à ces groupes organisés et « experts » dans l'art d'extorquer de l'argent par toutes sortes de moyens.

C'est un concept très important que nous mettons de l'avant ici. Le sénateur Nolin connaît bien la question des réclamations ou dommages dans un procès civil. En fait, nous avons devant nous toute une série d'approches différentes que nous souhaitons intégrer au Code criminel. Nous parlons ici de dommages immatériels, alors que l'article 738(1) parle de biens. Les biens sont matériels alors que la cote de crédit ou les antécédents en matière de crédit sont immatériels.

Le sénateur Angus : Non, elle parle des coûts directs liés au dédommagement des éléments immatériels. C'est différent.

Le sénateur Joyal : C'est très différent. C'est pourquoi j'attire l'attention du ministre et votre attention, à vous, honorables sénateurs, sur cette question. En principe, je n'y suis pas opposé, mais comment peut-on l'évaluer? Comment peut-on le formuler? Quelles sont les conséquences parallèles?

À mon avis, ce sont des questions très importantes. Je crois que nous devrions entendre les autres témoins sur le sujet parce que j'estime que c'est un élément important du projet de loi.

Le sénateur Angus : Si je comprends bien, c'est une peine additionnelle. Nous avons déjà des peines d'emprisonnement plutôt sévères. Ce dédommagement est en quelque sorte une sanction additionnelle et, par conséquent, j'imagine qu'elle se veut dissuasive. C'est essentiellement ce à quoi servent les peines; elles doivent dissuader les criminels et les encourager à ne pas commettre le crime envisagé.

Je crois que ce que vous dites n'est pas très clair et que ces coûts directs sont probablement insignifiants dans la plupart des cas. Selon ce que j'ai entendu au Comité des banques, on dit

credit agencies — in the experience we have seen at the Banking Committee — are much worse than that. You have to hire lawyers. It takes seven years of no unpaid bills to wipe your slate clean.

I do not think the Criminal Code should be getting involved in that area. I do not know if that is your point, but clearly we are into an area that is worthy of further examination.

Senator Joyal: I have a question about the concept of reasonable inference on page 7 of Bill S-4, the proposed new section 402.2. Could you give us an indication where other sections of the code would help us to understand what "reasonable inference" means?

Ms. Klineberg: The best example for an offence that is framed in that same way is section 351 of the Criminal Code, which is the offence for possession of housebreaking instruments.

Senator Baker: Breaking and entering to commit a crime is an indictable offence. Of course, that is in the tools.

Ms. Klineberg: I believe there may be one or two more, but we usually turn to section 351 as the prime example because this particular offence has been interpreted by the Supreme Court of Canada in the case of *Holmes* back in 1988, I believe. The Supreme Court interpreted that phrase in circumstances giving rise to a reasonable inference that the person or that the instrument had been used or was intended to be used. The Supreme Court said, in the criminal law —

Senator Joyal: To which case are you referring?

Ms. Klineberg: The *Holmes* case.

The Supreme Court interpreted that phrase as actually requiring the normal criminal standard of proof beyond a reasonable doubt that the accused person actually intended to use the instruments. Even though it is phrased as "circumstances giving rise to a reasonable inference," the courts said that any reasonable inference still, in the criminal law, has to be proof beyond a reasonable doubt that the person actually had the intention.

Senator Joyal: Therefore, you still have to prove the intention?

Ms. Klineberg: Yes. However, we sometimes see much interest on the part of police or prosecutors in this type of formulation for offences because, while any criminal offence can be proved on the basis of inferences, proof beyond a reasonable doubt of a person's intention can still be made out by circumstantial evidence and inferences drawn from circumstantial evidence. Sometimes, law

qu'Equifax impose des frais de 50 $, mais les coûts réels en cause pour Equifax et d'autres agences de crédit sont beaucoup plus élevés. Vous devez embaucher des avocats. Il faut compter sept années sans dettes impayées pour rétablir un dossier de crédit.

Je ne crois pas que le Code criminel devrait s'engager dans cette voie. Je ne sais pas si c'est ce que vous voulez dire, mais il est évident que nous ouvrons la porte à quelque chose que nous devons examiner très attentivement.

Le sénateur Joyal : J'ai une question au sujet de l'expression « permettent de conclure raisonnablement » qui figure à la page 7 du projet de loi S-4, dans le nouvel article 402.2 proposé. Pouvez-vous nous indiquer si d'autres articles du code nous aideraient à comprendre cette expression?

Mme Klineberg : Le meilleur exemple d'une infraction libellée de la même façon se trouve à l'article 351 du Code criminel, soit une infraction pour possession d'outils de cambriolage.

Le sénateur Baker : Entrer par effraction afin de commettre un crime est une infraction criminelle. Évidemment, tout se trouve dans les outils.

Mme Klineberg : Je crois qu'il peut y avoir un ou deux exemples de plus, mais généralement c'est l'article 351 que nous évoquons comme principal exemple puisque cette infraction particulière a été jugée par la Cour suprême du Canada dans l'affaire *Holmes*. Je crois que c'était en 1988. En effet, la Cour suprême a interprété cette expression de la façon suivante : des circonstances qui ont permis de conclure raisonnablement que la personne avait l'intention d'utiliser les outils ou que les outils avaient été effectivement utilisés dans l'intention de commettre une infraction criminelle. La Cour suprême a indiqué que, selon le droit criminel...

Le sénateur Joyal : À quelle affaire faites-vous référence?

Mme Klineberg : L'affaire *Holmes*.

Dans cette affaire, la Cour suprême a interprété cette expression comme exigeant que la norme criminelle de la preuve hors de tout doute raisonnable conclut que la personne accusée avait réellement l'intention d'utiliser les outils. Bien que formulée de la façon suivante : « des circonstances qui permettent de conclure raisonnablement », les tribunaux ont statué que, en droit criminel, le seul sens possible de cette expression est une conclusion qui prouve hors de tout doute raisonnable que la personne avait vraiment l'intention de commettre une infraction.

Le sénateur Joyal : Par conséquent, vous devez tout de même prouver l'intention de commettre l'infraction?

Mme Klineberg : Oui. Cependant, nous constatons parfois que, dans le cas des infractions, la police ou les avocats sont plus intéressés par ce type de formulation car, bien qu'une infraction criminelle puisse être prouvée par inférence, la preuve hors de tout doute raisonnable de l'intention d'une personne peut quand même être démontrée par des preuves circonstancielles et des

enforcement and prosecutors like this formulation of an offence because it builds the notion of the inference right into the offence in the way it is drafted.

Nonetheless, it is interpreted as if it had been written that the person intended to use the instrument or the information. It is a different way of saying the same thing.

Senator Joyal: Yes, however the word "circumstances" would be probably the proof to be made to the court to draw the intention or to support the intention.

Ms. Klineberg: Right, but that is the case no matter how you draft an offence. An offence will always be proved on the basis of inferences that we draw from circumstances. Unless you actually have a wiretap, for instance, and a person who says, "This is what I intend to use this information for," you will be asking the court to be concluding proof on the basis of inferences that they draw from the circumstances, in most cases.

Senator Joyal: Finally, on the issue of the definitions that were raised at the beginning on proposed new section 56.1(3): "For the purposes of this section, "identity document" means a Social Insurance Number card. . . ." and so forth.

I receive my income tax file from the government, which has my insurance number and personal information, and I file it. The bank might ask for my income tax declaration, for instance, to get credit, a loan or a mortgage or whatever I want to deal with, financially. Since it is a government document, why is it not covered in 56.1(3)?

As Senator Fraser has mentioned, "identity document" is defined as being issued or purported to be issued by a government department. The document I receive from the income tax department is issued by a government department, and it has very private information that could give anyone the opportunity to steal any identity.

Why is such a document excluded from this definition? Is it because it is limitative in terms of the enumeration you give in the definition?

Ms. Klineberg: Yes. As the minister indicated earlier, this offence has a very low threshold for conviction because it does not require proof that there was any intention on the person's part to use the document in any sort of fraudulent way. Mere possession or transfer of these documents is sufficient to make out the offence, unless, of course, the person has a lawful excuse or fits into one of the enumerated grounds. It has a very low threshold for proof of this offence.

Due to the low threshold, it was our view — and for Charter reasons, in particular — that the class of documents had to be very limited. It is similar to a trade-off: The lower we want to go

conclusions tirées de preuves circonstancielles. Il arrive que les services d'exécution de la loi et les avocats préfèrent cette formulation d'une infraction parce que, la façon dont elle est rédigée, elle intègre directement la notion d'inférence à l'infraction.

Néanmoins, on l'interprète comme s'il était écrit que la personne avait l'intention d'utiliser les outils ou l'information à sa disposition. C'est une façon différente de dire les choses.

Le sénateur Joyal : Oui, cependant, le mot « circonstances » constituerait probablement la preuve à démontrer devant le tribunal pour déduire l'intention ou pour appuyer l'intention.

Mme Klineberg : Exact, mais c'est généralement le cas, peu importe la façon dont vous rédigez l'infraction. Une infraction devra toujours être prouvée en se fondant sur les inférences déduites des circonstances. À moins d'avoir mis une personne sur écoute, par exemple, ou qu'une personne affirme « J'ai l'intention d'utiliser ces renseignements pour faire ceci ou cela », dans la plupart des cas, vous devrez demander au tribunal de conclure la preuve à la lumière des inférences fondées sur les circonstances.

Le sénateur Joyal : Pour terminer, au sujet de la question des définitions soulevées au début du nouveau paragraphe 56.1(3) : « Pour l'application du présent article, « pièce d'identité » s'entend de la carte d'assurance sociale [...] » et ainsi de suite.

Disons que je reçois mon dossier d'impôt sur le revenu du gouvernement, sur lequel figurent mon n^{o} d'assurance sociale et des renseignements personnels, et que je le classe. La banque peut, par exemple, me demander ma déclaration d'impôt sur le revenu pour décider de m'accorder un crédit, un prêt ou une hypothèque, ou toute autre aide financière. Comme il s'agit d'un document du gouvernement, pourquoi n'est-il pas visé par le paragraphe 56.1(3)?

Comme l'a signalé le sénateur Fraser, « la pièce d'identité » est définie comme étant une pièce délivrée ou paraissant délivrée par un ministère ou un organisme public gouvernemental. Le document que je reçois du ministère du Revenu est délivré par un ministère du gouvernement et contient des renseignements très personnels qui pourraient donner à quiconque la possibilité de voler une identité.

Pourquoi un tel document est-il exclu de cette définition? Est-ce en raison de l'énumération restrictive qu'en donne la définition?

Mme Klineberg : Oui. Comme le ministre l'a indiqué précédemment, dans le cas de cette infraction le seuil de déclaration de culpabilité est très bas parce qu'on n'exige aucune preuve de l'intention de la personne d'utiliser ce document de façon frauduleuse. La seule possession ou le seul transfert de ces documents suffit à prouver l'infraction à moins, bien sûr, que la personne n'avance une excuse légitime ou l'un des motifs énumérés. Le seuil de l'élément servant à prouver l'infraction est effectivement très bas.

En raison de ce seuil très bas, et à notre avis, pour des raisons liées à la Charte en particulier, cette catégorie de documents devait être très restreinte. C'est semblable à une négociation. Si

in terms of the fault element for the offence, the clearer, narrower and more circumscribed we really have to be in terms of what constitutes an offence.

In this particular offence, we were trying to get at documents that are used by individuals for identification purposes — not documents that contain information, not their financial statements, not a number of other documents you might receive from the government that contain a number of pieces of information of a private or confidential nature, but the foundational identity documents that govern individuals' relationships with the government and the private sector. These are the documents that form the basis of what identity is. In the interests of ensuring the maximum likelihood of this offence being found to be constitutional, we tried very hard to limit the types of documents to those core identity documents that regulate all of our interactions with the private sector and the public sector.

Senator Joyal: What about a death certificate? You have a birth certificate listed here, but a death certificate could be as useful for someone trying to re-establish the identity of someone as a birth certificate. In fact, sometimes it could be even more useful, for obvious reasons, because no one will claim that their identity was stolen.

Senator Angus: You are familiar with the electoral lists.

Senator Joyal: I am an old pro, like you.

A death certificate is a government document. There is no doubt about that. It is a provincial government. It is as useful and as needed by those who want to re-establish the identity of other people or claim the identity of other people as any other document. Why was the death certificate not included?

Ms. Klineberg: The honest answer is that it did not occur to us. We developed this list in consultation with a number of other government departments. We held consultations with a range of government departments that issue these sorts of documents. Together, we tried to determine the core documents that we should be including on this list. I can only imagine that death certificates did not occur to us. As you say, it is a provincial document. Everyone has their own birth certificate. None of us, as yet, have our own death certificate. I do not think it occurred to us. It seems to me as though it might be a valid addition to the list.

Senator Nolin: This type of crime is not limited to one province. It is international. It involves many jurisdictions. The cost of a law enforcement organization going through this type of investigation could be a deterrent to the implementation of Bill S-4. The minister would probably have been the right person to answer this. As we all know, the provinces will have to operate

nous voulons situer le seuil de l'élément de preuve de l'infraction au niveau le plus bas possible, plus notre définition d'une infraction doit être claire, restreinte et circonscrite.

Dans le cas de cette infraction particulière, nous tentons de nous limiter aux documents utilisés par des personnes à des fins d'identification — donc pas de documents contenant de l'information, pas d'états financiers ni aucun autre document que vous pourriez recevoir du gouvernement et susceptible de contenir des éléments d'information de nature privée ou confidentielle, mais bien des pièces d'identité de base sur lesquelles se fondent les relations entre, d'une part, les particuliers et, d'autre part, le gouvernement et le secteur privé. Il s'agit de documents qui constituent le fondement même de l'identité. De plus, pour nous assurer d'un maximum de vraisemblance que cette infraction soit jugée constitutionnelle, nous avons déployé beaucoup d'efforts pour limiter le type de documents aux pièces d'identité essentielles qui régissent toutes nos interactions avec le secteur privé et le secteur public.

Le sénateur Joyal : Qu'en est-il d'un certificat de décès? Votre liste parle du certificat de naissance, mais un certificat de décès pourrait être utile à toute personne qui cherche à rétablir l'identité d'une personne par un certificat de naissance. En fait, il pourrait parfois s'avérer plus utile et ce, pour des raisons évidentes, parce que personne n'ira se plaindre que son identité a été volée.

Le sénateur Angus : Vous connaissez bien les listes électorales.

Le sénateur Joyal : Oui, je suis un vieux routier, tout comme vous.

Un certificat de décès est un document délivré par le gouvernement. Aucun doute là-dessus. En fait, c'est un document délivré par un gouvernement provincial. Il est tout aussi utile et nécessaire aux personnes qui désirent rétablir l'identité d'une autre personne ou qui prétendent à l'identité d'une autre personne que tout autre document. Alors pourquoi ce certificat n'est pas inclus dans la liste des documents?

Mme Klineberg : Honnêtement, c'est que nous n'y avons pas pensé. Nous avons établi cette liste en consultant un certain nombre de ministères. Nous avons consulté tout un éventail de ministères qui délivrent ce genre de documents. Ensemble, nous avons essayé de déterminer les principaux documents à inclure dans cette liste. Je peux tout simplement vous dire qu'il ne nous est pas venu à l'idée d'y inclure les certificats de décès. Comme vous le savez, c'est un document délivré par une province. Tout le monde a un certificat de naissance. Aucun d'entre nous ne possédons, à ce jour, un certificat de décès. C'est pourquoi nous n'y avons pas pensé. Toutefois, à mon avis, ce serait un ajout très justifié à la liste.

Le sénateur Nolin : Ce type d'acte criminel n'est pas limité à une province. C'est une infraction à l'échelle internationale qui, de ce fait, concerne de nombreuses compétences. Les coûts associés à une enquête de ce type menée par un organisme d'application de la loi pourraient constituer un frein à la mise en œuvre du projet de loi S-4. En fait, le ministre serait probablement la bonne

the system. What will we do to help them? Do you have in mind some type of information sharing to help them do the job?

Ms. Klineberg: As far as I know, nothing of the nature of an information-sharing database is being contemplated at this time. In terms of additional funding for law enforcement, that is something I would not want to speak to; I am sorry.

The Chair: We can write to the minister, or you could just convey to the minister that question, which might be a little faster. It would be something we would be interested in learning.

Senator Nolin: There is no point in making laws if we are just creating a bigger monster for those who have to enforce them.

The Chair: As we were reminded earlier today in another context, the RCMP is the police force in many provinces. That is not even provincial. That is direct federal responsibility.

Senator Nolin: I thought the minister would have been the right person to answer that. That is why I stopped there.

Senator Milne: I have a supplementary to what Senator Nolin has just asked, but also a further question, if I may.

Will this bill in any way force companies to notify customers when their identity has been stolen? Is there anything in the bill that will force companies to let people know?

Ms. Klineberg: No. We would not use the Criminal Code for that sort of mechanism.

Senator Milne: This is where the data bank would come in handy.

Ms. Klineberg: I know that matter has been debated in consideration of amendments to the Personal Information Protection and Electronic Documents Act, PIPEDA. Unfortunately, I am not up to date on the status of their decision making on that particular issue. If you like, I would be happy to convey that to my colleagues at Industry Canada.

The Chair: I would like that because I want to know the justification for saying that this is not something we would do in the criminal law. In a sense, this goes back to our discussion about reckless earlier.

Senator Milne: It goes back to enforcement.

The Chair: When people know that serious personal information has been stolen, why should it not be a criminal offence to fail to notify the person to whom the information refers, since so much else is being made criminal, and I think rightly so, from all we have heard.

personne qui pourrait répondre à cette question. Comme nous le savons tous, il reviendra aux provinces d'assurer l'application du système. Qu'entendons-nous faire pour les aider? Avez-vous réfléchi à certains types d'échange d'information qui pourraient les aider à faire leur travail?

Mme Klineberg : À ma connaissance, rien n'a été envisagé pour le moment quant à la nature d'une base de données commune aux fins d'échange d'information. Pour ce qui est du financement additionnel aux fins de l'application de la loi, c'est une question que je ne veux pas aborder; je suis désolée.

La présidente : Nous pouvons écrire au ministre sur le sujet ou peut-être pourriez-vous tout simplement transmettre cette question au ministre, ce qui serait plus rapide. C'est un élément sur lequel nous aimerions en savoir davantage.

Le sénateur Nolin : Il ne sert à rien d'adopter des lois si nous ne faisons que créer un monstre encore plus gros pour ceux qui ont la responsabilité d'appliquer ces lois.

La présidente : Comme on nous l'a rappelé plus tôt aujourd'hui dans un autre contexte, la GRC est le service de police de nombreuses provinces. Ce n'est même pas un service provincial; il relève directement du gouvernement fédéral.

Le sénateur Nolin : Je croyais que le ministre serait le mieux placé pour répondre à cette question. C'est pourquoi j'ai arrêté là.

Le sénateur Milne : J'aurais quelque chose à ajouter à ce que vient de dire le sénateur Nolin, et j'aurais une autre question, si vous me permettez.

Est-ce que le projet de loi obligerait les entreprises à informer les consommateurs du vol de leur identité? Y a-t-il quelque chose de prévu au projet de loi pour forcer les entreprises à informer les gens?

Mme Klineberg : Non. Nous n'utiliserons pas le Code criminel pour mettre en place ce type de mécanisme.

Le sénateur Milne : C'est là que la banque de données serait pratique.

Mme Klineberg : Je sais que cette question fait déjà l'objet de débats à savoir s'il faudrait modifier la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE). Malheureusement, je ne sais pas où en sont les discussions ni si des décisions ont été prises à cet égard. Si vous le souhaitez, il me ferait plaisir d'en parler avec mes collègues d'Industrie Canada.

La présidente : J'apprécierais, car j'aimerais savoir les raisons pour lesquelles il ne faudrait pas l'inclure au droit criminel. D'une certaine façon, ça nous ramène à la discussion que nous avons eue plus tôt sur l'insouciance.

Le sénateur Milne : Ça nous ramène à l'application de la loi.

La présidente : Quand quelqu'un sait que des renseignements personnels importants ont été volés, pourquoi le fait de ne pas informer la personne victime du vol de ces renseignements ne constituerait pas une infraction criminelle, puisque tant de choses constituent des crimes, et à juste titre, selon ce que nous avons entendu?

Senator Milne: There is an example in case law about identity theft. This is the case of *R. v. Boyle*, 2005. It was, I believe, out in British Columbia. Mr. Boyle was convicted of fraudulently impersonating a man who was dead with intent to gain an advantage for himself. This is contrary to section 403(*a*) of the Criminal Code. He appealed his conviction. It was not successful. In this case, the trial judge ruled it was only required to find that the appellant had the intent to gain an advantage by impersonating someone else. That is already in the Criminal Code. In your opinion, how would this bill change that?

Ms. Klineberg: That, as you have correctly noted, is the offence of personation, which is what we could call the end stage of the identity-theft spectrum. It has been in the Criminal Code, I think, since 1892, but I would have to verify that for you. Various forms of fraud, as well, cover the end stage where people pretend to be someone else, for instance, to take out a fraudulent mortgage on someone else's piece of property. The end stage of identity crime is already covered by the Criminal Code.

One of the amendments that we have not talked about yet is that the offence of personation in Bill S-4 will actually be renamed "identity fraud." The new offences that are being created in Bill S-4 apply at the early stage of the identity-theft spectrum. They are offences that target the gathering of information with intention to use it later, the trafficking in the information, being reckless knowing that someone else would use it later. The new offences cover the earlier stages of the identity crime. The offences we already have in the Criminal Code cover those quite nicely. We will rename personation "identity fraud" and create some identity-theft offences, and the hope is that this will create a more coherent understanding of the full range of identity-theft activities or identity-crime activities, you could say.

A great deal of inconsistency in the use of terminology exists in this area, which is also one of the reasons we have renamed personation to "identity fraud." If each one of us were to give our definitions of identity theft, we all might define it slightly differently. Some people use the term identity theft to encompass personation when they are actually just different phases of the same activity.

Bill S-4 fills the gaps, as the minister said. The gaps are at the early stages: the collection of the information, the manipulation of the information and the trafficking of information. We have heard numerous times from law enforcement that they will uncover an operation where they have a warehouse full of documents, identity profiles and forged documents, but they cannot prove that any of them had been used yet. Had some of those documents been used, you might be at the stage of personation or fraud, but in advance of them being used, currently there is not all that much that the law can do. Bill S-4 fills that gap.

Le sénateur Milne : Il existe un cas de jurisprudence concernant le vol d'identité. Il s'agit de l'affaire *R. c. Boyle*, 2005. Je crois que ça s'est passé en Colombie-Britannique. M. Boyle a été condamné pour s'être fait frauduleusement passer pour un homme mort avec l'intention d'obtenir un avantage pour lui-même. Cela est contraire à l'alinéa 403*a*) du Code criminel. Il a interjeté appel du verdict de culpabilité. L'appel a été rejeté. Le juge qui présidait l'audience a établi qu'il suffisait de déterminer que l'accusé avait l'intention d'obtenir un avantage en se faisant passer pour quelqu'un d'autre. Tout ça est déjà dans le Code criminel. Selon vous, en quoi le projet de loi changerait quelque chose?

Mme Klineberg : Comme vous l'avez correctement souligné, ceci fait référence à la supposition de personne, qui est l'étape finale du cycle du vol d'identité. Elle a été introduite au Code criminel, je crois, en 1892, mais il faudrait que je vérifie. D'autres types de fraudes couvrent-elles aussi l'étape finale, où les gens prétendent être quelqu'un d'autre, par exemple, pour contracter un faux prêt hypothécaire relativement à la propriété de quelqu'un d'autre. L'étape finale du vol d'identité est déjà couverte par le Code criminel.

L'un des amendements dont nous n'avons pas encore parlé concerne l'infraction de supposition de personne qui, dans le projet de loi S-4, serait renommée la « fraude à l'identité ». Les nouvelles infractions amenées par le projet de loi S-4 toucheraient les premières étapes du cycle du vol d'identité. Ces infractions touchent notamment la collecte de renseignements dans l'intention de s'en servir plus tard, le trafic de renseignements, et l'insouciance de savoir que quelqu'un s'en servira plus tard. Les nouvelles infractions concerneraient les premières étapes du vol d'identité, même si elles sont déjà plutôt bien couvertes par les infractions actuellement prévues au Code criminel. Nous voulons renommer la supposition de personne la « fraude à l'identité » et créer de nouvelles infractions relatives au vol d'identité dans l'espoir d'améliorer la compréhension des processus impliqués dans le vol d'identité et les crimes liés à l'identité, si l'on peut dire.

Il existe beaucoup d'incohérences dans l'utilisation de la terminologie dans ce domaine, ce qui explique aussi pourquoi nous voulons renommer la supposition de personne la « fraude à l'identité ». Si chacun d'entre nous avait à donner une définition de ce qu'est le vol d'identité, nous arriverions probablement à des résultats légèrement différents. Certains parlent de vol d'identité plutôt que de supposition de personne, alors qu'il s'agit en fait de la même activité, mais à deux étapes différentes.

Le projet de loi S-4 comble les lacunes, comme l'a dit le ministre. Les lacunes concernent les premières étapes : la collecte, la manipulation et le trafic de renseignements. Nous avons entendu à maintes reprises des organismes d'application de la loi dire qu'ils allaient bientôt dévoiler une opération dans le cadre de laquelle ils auraient accumulé un entrepôt de documents, de profils d'identité et de documents contrefaits, mais ils n'ont pas réussi à prouver qu'aucun de ces documents n'avait été utilisé. Si ces documents avaient été utilisés, on parlerait alors de l'étape de la supposition de personne ou de fraude, mais comme ils n'ont pas encore été utilisés, il n'y a rien à faire compte tenu de la loi. Le projet de loi S-4 comblerait cette lacune.

Senator Joyal: I apologize to my colleagues.

What about the biometric documents that the government would develop to cross borders? We know those sorts of documents will be used and developed more in the future because the technology is proceeding.

Why do you not have a definition included that would cover that possible development? The development is underway. If we are to address that problem in the future, why do we not cover that here?

Ms. Klineberg: The short answer is that we did try to take into account the NEXUS pass and the CANPASS Air in the definition in proposed new section 56.1(3). We included a passport, but also "a document that simplifies the process of entry into Canada." We were aware of the NEXUS card, and we tried to cover it.

With respect to future documents created, the information contained in those documents would fall within the definition of "identity information" in proposed new section 402.1. That information would be covered and included in the offences of "identity theft" and "trafficking in identity information."

You are correct to point out that new documents would not be included in the document offence unless a coordinating amendment was made to the Criminal Code at the same time as passage of that legislation. We had been advised to give this offence the greatest chance of surviving a constitutional challenge; we had to be very circumscribed in the scope of documents included. To leave room for new documents that may be created one day would introduce a degree of vagueness that we were concerned might make the offence more vulnerable.

Proposed new section 56.1 is the only offence where we have received criticism from legal associations on that very point that it does not contain much on mental state. It is really only possession of these documents. They are not contraband documents. We all have them. At any given time, I might have my mother's passport, et cetera.

A risk exists with this particular offence. You may hear that if you have legal associations testify before you. We have closed off that list solely for the purpose of giving it the greatest chance of surviving.

Senator Joyal: I understand that the bill, as drafted, does not cover the case whereby someone fabricates an identity with elements taken from various sources, which is creating a new person not.

Senator Baker: That is interesting.

Ms. Klineberg: The offence of personation, which is an existing offence in the Criminal Code, is limited to a person living or dead.

Le sénateur Joyal : Je m'excuse auprès de mes collègues.

Qu'en est-il des documents biométriques que le gouvernement compte développer pour quand vient le temps de traverser les frontières? Nous savons que ce type de documents pourra être développé et utilisé dans le futur puisque la technologie le permet.

Pourquoi n'auriez-vous pas une définition qui couvrirait la création éventuelle de ces documents? Les travaux sont en cours. Si nous sommes pour nous attaquer à ce problème dans le futur, pourquoi ne pas en tenir compte?

Mme Klineberg : Pour répondre brièvement, disons seulement que nous avons essayé de tenir compte du laissez-passer NEXUS et de la carte CANPASS dans la définition proposée au nouveau paragraphe 56.1(3). Nous y parlons de passeport, mais aussi de « tout document simplifiant les formalités d'entrée au Canada ». Nous connaissions le laissez-passer NEXUS, et nous avons essayé d'en tenir compte.

Pour ce qui est des documents qui seront créés, les renseignements qu'ils pourraient contenir correspondraient à la définition de « renseignement identificateur » proposée dans le nouvel article 402.1. Ces renseignements seraient protégés par les infractions relatives au « vol d'identité » et au « trafic de renseignements identificateurs ».

Vous faites bien de souligner que les nouveaux documents ne correspondraient pas aux infractions prévues, à moins qu'il y ait un amendement prévu au Code criminel au moment où la loi sera adoptée. On nous a conseillé de donner à cette infraction le plus de chances possible de survivre à une contestation constitutionnelle; il nous fallait donc limiter au maximum le type de documents inclus. De vouloir laisser plus de place aux nouveaux documents qui pourraient un jour être créés nous aurait obligés à être beaucoup moins précis dans nos propos, mais nous avions peur de rendre ainsi cette infraction plus vulnérable.

Seul le nouvel article 56.1 a été quelque peu critiqué par les associations juridiques, et seulement parce qu'il ne faisait pas mention de l'état mental. On n'y parle que de la possession de documents. Il n'est pas question de documents contrefaits. Nous pouvons tous en avoir. À tout moment, je pourrais me promener avec le passeport de ma mère, et cetera.

Cette infraction bien précise peut constituer un risque. C'est ce que vous entendrez si vous demandez à des associations juridiques de témoigner devant vous. Nous avons limité cette liste seulement dans le but de lui laisser une chance de survie.

Le sénateur Joyal : Ce que je comprends, c'est que le projet de loi, de la façon dont il est rédigé, ne couvre pas les cas où quelqu'un fabriquait une nouvelle identité à partir d'éléments provenant de différentes sources, créant ainsi une nouvelle personne.

Le sénateur Baker : C'est intéressant.

Mme Klineberg : L'infraction de supposition de personne, qui existe actuellement au Code criminel, se limite aux personnes vivantes ou mortes.

We were very aware of this concern during the creation of the new offences — identity theft, trafficking in identity information and the document offence. When people read the bill, I do not think they tweak to what we have done to address this issue. You will notice the phrase "an identity document that relates or purports to relate, in whole or in part, to another person."

When you go to proposed new section 402.1, it says the definition of "identity information means any information . . . of a type that is commonly used alone or in combination with other information to identify or purport to identify an individual."

We have specifically used those words to signify that even if the person is not a real person, but the information is presented as though it were relating to a real person, it should be covered.

Some people who read this legislation, if they are not familiar with reading criminal legislation, might not pick up that that is what those words are meant to do. However, we clearly intend to cover wholly fictitious identities as well as composites where some fictitious information is combined with information belonging to a real person.

The Chair: I should point out that Senator Joyal is "deeply" familiar with reading criminal legislation.

Ms. Klineberg: That is true.

Senator Baker: She did not mean him.

Senator Nolin: You raised my concern when talking about carrying the passport of your mother. Some Canadians are listening to us and — I am sure — are very nervous in hearing your answer. I assume you would be protected when Bill S-4 uses the language "without a lawful excuse." Is that what you mean by a lawful excuse?

Ms. Klineberg: We have done even better. If you look at proposed new section 56.1(2)(*c*), it says, "with the consent of the person to whom the identity document relates."

Senator Nolin: That means you need to prove the consent of someone. If you have your mother's passport in your purse, and she cannot give her consent, but needs a passport to go through immigration, do you have a lawful excuse?

Ms. Klineberg: Yes.

Senator Nolin: Okay, good.

Ms. Klineberg: The lawful excuse is the backup if those explicitly listed exclusions do not apply.

The Chair: Under that same proposed subsection, I assume you would be the "person authorized to consent," if you are ushering your mother through customs.

Nous étions très conscients de ce problème quand nous avons créé les nouvelles infractions — le vol d'identité, le trafic de renseignements identificateurs et l'infraction relative aux pièces d'identité. Je ne crois pas que les gens se rendent compte des légères modifications que nous avons apportées au projet de loi pour régler ce problème. Vous remarquerez le passage « une pièce d'identité qui concerne ou paraît concerner, en totalité ou en partie, une autre personne ».

Si vous vous rendez à l'article 402.1, vous verrez que « renseignement identificateur s'entend de tout renseignement [...] d'un type qui est ordinairement utilisé, seul ou avec d'autres renseignements, pour identifier ou pour viser à identifier une personne physique ».

Nous avons volontairement utilisé ces mots pour dire que même si une personne n'est pas réelle, mais que les renseignements sont présentés comme si cette personne existait vraiment, la loi devait s'appliquer.

Une personne qui lit cette loi mais qui n'a pas l'habitude des lois criminelles ne saisira pas tout le sens de ces mots. Toutefois, nous voulions couvrir toute identité fictive ou mixte, auquel cas des renseignements fictifs sont combinés à des renseignements appartenant à une vraie personne.

La présidente : J'aimerais faire remarquer que le sénateur Joyal est passé maître dans la lecture des lois criminelles.

Mme Klineberg : C'est vrai.

Le sénateur Baker : Elle ne parlait pas de lui.

Le sénateur Nolin : Je me pose des questions depuis que vous avez parlé de transporter le passeport de votre mère. Certains Canadiens nous écoutent en ce moment, et — je suis certain — ils ont très hâte d'entendre votre réponse. Je présume que vous seriez protégée étant donné que le projet de loi S-4 utilise les mots « sans excuse légitime ». Est-ce que c'est ce que vous voulez dire par excuse légitime?

Mme Klineberg : Nous avons fait encore mieux. Si vous regardez l'alinéa 56.1(2)*c*), on y lit « avec le consentement de la personne visée par la pièce d'identité ».

Le sénateur Nolin : Ça veut dire que vous devez prouver le consentement de la personne. Si vous transportez le passeport de votre mère dans votre sac à main, et que bien qu'elle ne soit pas en mesure de donner son consentement, elle a besoin d'un passeport pour passer l'immigration, avez-vous une excuse légitime?

Mme Klineberg : Oui.

Le sénateur Nolin : D'accord, ça va.

Mme Klineberg : L'excuse légitime a été prévue pour les cas où les exclusions citées ne s'appliquent pas.

Le président : Dans le même alinéa, je présume que vous seriez la « personne autorisée à donner son consentement » si vous avez à faire passer les douanes à votre mère.

Senator Wallace: Ms. Klineberg, you have mentioned that there are new offences in the bill dealing with the use of credit cards and credit card data. There is no mention of debit cards or ATM cards though, which are obviously somewhat similar. Is there a particular reason why they were not included?

Ms. Klineberg: This is another of these unfortunate situations where we put a definition in one part of the code that is slightly removed from the offences. Section 321 of the Criminal Code has a definition of credit card that includes debit cards.

Senator Wallace: Okay.

Ms. Klineberg: It says:

> "Credit card" means any card . . . distributed for the purpose of being used . . .
>
> (*b*) in an automated teller machine, a remote service unit or a similar automated banking device to obtain any of the services offered through the machine, unit or device; . . . .

We have the definition in section 321 of the Criminal Code rather than having to use both "credit card" and "debit card" each time it appears in an offence. It is simply a drafting convention, but unfortunately I have noticed that again it seems to be confusing.

Senator Joyal: That definition certainly makes it clearer.

Ms. Klineberg: Yes. Without any doubt whatsoever, law enforcement, Crown prosecutors and the courts are well aware that debit cards are covered by the law even though if you were simply to read the offences, you might not think that is the case.

The Chair: Why then do you refer to "credit card number" and "debit card number" in proposed section 402.1?

Ms. Klineberg: This is what happens to a Criminal Code after more than 100 years. It is quite unfortunate in some ways.

The definition in section 321 applies only in Part 9 of the Criminal Code.

The Chair: Okay.

Ms. Klineberg: We would have had to say as well that credit cards include —

The Chair: No, that is fine. It is not good, but it is a comprehensible answer.

Senator Wallace: It is picked up in the definition. That is a clean answer. Thank you.

The Chair: It was an extremely interesting session. Thank you, Ms. Klineberg. It is not often that one person is willing to sit and take many technical questions. I congratulate you. You did very well indeed.

Le sénateur Wallace : Madame Klineberg, vous avez dit que le projet de loi comprenait de nouvelles infractions concernant l'utilisation des cartes de crédit et des données relatives à une carte de crédit. Il n'y a aucune mention des cartes de débit ni des cartes de guichet automatique cependant, qui sont pourtant quelque peu similaires. Y a-t-il une raison pourquoi il n'en est nullement mention?

Mme Klineberg : Il s'agit d'une des situations malencontreuses où la définition donnée dans une partie du code nous évite de devoir tout répéter dans les infractions. L'article 321 du Code criminel donne une définition de carte de crédit qui inclut les cartes de débit.

Le sénateur Wallace : D'accord.

Mme Klineberg : La voici :

> « carte de crédit » désigne notamment les cartes [...] délivrés afin :
>
> b) soit de permettre l'accès, par un guichet automatique, un terminal d'un système décentralisé ou un autre service bancaire automatique, aux différents services qu'offrent ces appareils.

La définition se trouve donc à l'article 321 du Code criminel, ce qui nous évite d'avoir à répéter « carte de crédit » et « carte de débit » chaque fois qu'il en est question. Il s'agit simplement d'une convention de rédaction, mais malheureusement, je remarque que ça peut parfois porter à confusion.

Le sénateur Joyal : Cette définition clarifie beaucoup les choses.

Mme Klineberg : Oui. Il ne fait aucun doute que les organismes d'application de la loi, les procureurs de la Couronne et les tribunaux savent très bien que les cartes de débit sont couvertes par la loi, même si ça ne semble pas être le cas à la simple lecture des infractions.

La présidente : Pourquoi alors parlez-vous de « n^{o} de carte de crédit ou de débit » à l'article 402.1?

Mme Klineberg : C'est ce qui arrive à un code criminel après plus de 100 ans. Il y a parfois des incohérences.

La définition de l'article 321 ne s'applique qu'à la partie 9 du Code criminel.

La présidente : D'accord.

Mme Klineberg : Il faudrait aussi dire que les cartes de crédit comprennent...

La présidente : Non, ça va. Ce n'est pas l'idéal, mais c'est une réponse compréhensible.

Le sénateur Wallace : C'est tiré de la définition. C'est une réponse claire. Merci.

La présidente : Cette séance a été extrêmement intéressante. Merci, madame Klineberg. Ce n'est pas tous les jours que quelqu'un accepte de venir répondre à toutes nos questions techniques. Je vous félicite. Vous avez très bien relevé le défi.

Honourable senators, we shall meet again in this room at 10:45 a.m. tomorrow morning to continue our study of this bill.

(The committee adjourned.)

OTTAWA, Thursday, May 14, 2009

The Standing Senate Committee on Legal and Constitutional Affairs, to which was referred Bill S-4, An Act to amend the Criminal Code (identity theft and related misconduct), met this day at 10:47 a.m. to give consideration to the bill.

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

[*English*]

The Chair: The Standing Senate Committee on Legal and Constitutional Affairs will continue its study of Bill S-4. We have the great pleasure of welcoming as our first witness Mr. David McMahon, who is Advisor, National Security — Bell Canada, and who is representing the Information Technology Association of Canada. In other words, he understands how the crooks do what they do, and he is here to explain it to us.

[*Translation*]

Mr. McMahon, we are pleased to have you with us. I believe you know how things work. You will make your opening remarks, and then, we will move on to questions. The floor is yours.

David McMahon, Advisor, National Security — Bell Canada, Information Technology Association of Canada: Thank you very much for inviting me here today. I am representing the Information Technology Association of Canada. They asked me to speak on the subject of identity theft. Specifically, my area of expertise is looking at the cyber threat over the last 20 years and the technological focus as it is implicated within identity theft.

To summarize the rather sophisticated concept around identity theft, it has been around in some form for hundreds of years, if not thousands. What makes it different in 2009 are how technology has implicated itself and the growing importance of technology in facilitating identity theft on vast scales.

Within the centre of a technologically assisted identity theft ring is money. There are types of identity theft that are not associated with money, but they are few and far between, considering that nearly everything bad that happens on the Internet at this time has a financial goal at the other end. That is also to say that all the bad things that happen within cyberspace do not necessarily include identity theft. In some cases, criminals will look at trying to get at the money as fast as they can. If they can get at it by theft of goods and services, they will. If they have to, they will go after identity theft, and if they are able to acquire the identities of persons, they are able to fence those off in the global market.

Honorables sénateurs, nous nous rencontrerons de nouveau dans cette salle à 10 h 45 demain matin pour continuer notre étude du projet de loi.

(La séance est levée.)

OTTAWA, le jeudi 14 mai 2009

Le Comité sénatorial permanent des affaires juridiques et constitutionnelles, auquel a été déféré le projet de loi S-4, Loi modifiant le Code criminel (vols d'identité et inconduites connexes), se réunit aujourd'hui à 10 h 47 pour étudier le projet de loi.

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

[*Traduction*]

La présidente : Le Comité sénatorial permanent des affaires juridiques et constitutionnelles poursuit l'étude du projet de loi S-4. C'est avec beaucoup de plaisir que nous accueillons notre premier témoin, M. David McMahon, qui est conseiller à Sécurité nationale de Bell Canada et qui représente l'Association canadienne de la technologie de l'information. On pourrait donc dire qu'il comprend la façon d'agir des fraudeurs et il est ici pour nous l'expliquer.

[*Français*]

Monsieur McMahon, nous sommes heureux de vous recevoir. Je pense que vous comprenez la procédure. Nous vous demandons de faire une déclaration d'ouverture et ensuite nous passerons à la période des questions. La parole est à vous.

David McMahon, conseiller, Sécurité nationale — Bell Canada, Association canadienne de la technologie de l'information : Je vous remercie infiniment de m'avoir invité ici aujourd'hui. Je représente l'Association canadienne de la technologie de l'information. On m'a demandé de parler de la question du vol d'identité. Je suis plus particulièrement spécialisé dans l'évolution de la cybermenace au cours des 20 dernières années et les particularités technologiques du vol d'identité.

Pour résumer le concept complexe du vol d'identité, je vous dirai que ce problème existe depuis des centaines, voire des milliers d'années. Ce qui est différent en 2009, c'est le rôle joué dorénavant par la technologie, ce qui facilite de plus en plus le vol d'identité à grande échelle.

L'argent est au cœur du vol d'identité assisté par la technologie. Il existe des types de vol d'identité qui ne sont pas associés à l'argent, mais ils sont peu nombreux et peu fréquents, compte tenu du fait que presque tous les méfaits commis de nos jours à l'aide d'Internet sont mus par des motifs pécuniaires. Il faut ajouter cependant que tous les méfaits commis dans le cyberespace n'impliquent pas nécessairement le vol d'identité. Les criminels cherchent parfois à faire de l'argent le plus rapidement possible. S'ils doivent voler des biens et des services pour parvenir à leurs fins, ils le feront. Ils n'hésiteront pas non plus à recourir au vol d'identité. S'ils sont en mesure d'usurper l'identité d'une personne, ils n'hésiteront pas à s'en servir à l'échelle mondiale.

How does this generally occur in this day and age? The most traditional way, which you may have heard about, is credit card skimming, taking advantage of breaches that occur — surreptitious breeches, disclosures within various communities of interest, and also harvesting what people put up about themselves on the Internet. A typical example would be Facebook, where what people put up about themselves can be harvested and then used.

The other way, which is becoming much more prevalent, is the use of robot networks that infiltrate and harvest goods and services off people's computers, essentially taking over peoples' computers. The first modus operandi is to use those computers to generate money for organized crime. The second purpose is to take whatever identity they can accrue from those Trojanized computers and be able to peddle those off on the black market. A whole industry has developed within the criminal enterprises that, first, collects the information from bits and pieces through different means, and second, is then able to make use of it. The two are not necessarily connected. The people who collect the information are not necessarily the ones who use it.

Going after these criminal networks requires a two-tier approach: monitoring the people making the end use of personal identity and then going after those behind the scenes collecting the identity in the first place.

I am available to answer any specific questions you might have on a technological basis.

The Chair: You are faced with a group of people not including engineers and technological experts, but I am sure that we will have questions for you, Mr. McMahon.

Senator Wallace: Welcome here today, Mr. McMahon. Thank you for your comments. As you know, the focus of this committee and this hearing is Bill S-4. I am certainly not a techie when it comes to Internet technology and all the things you are well familiar with.

I will start off with an easy question, or at least easy from my perspective. With the issues that you are involved with and the technological challenges and the infiltration by organized crime and the impact that has on identity theft, which is a terrible scourge of our society, I am wondering what your reaction is to Bill S-4. How do you feel it responds to this problem we have?

Mr. McMahon: Having had a chance to look over the bill briefly and consult with my colleagues beforehand, I think part of the problem is solved or ameliorated by legal documents and the ability to prosecute people, especially within Canada. The other part is a technical solution.

Without speaking too directly to the legal aspects of it, I think it is important that we have instruments that allow prosecutors to bring people to account for things like having 1 million or 10,000 identities built up on their computer. Clearly something is not right. To give you an analogy, it is not illegal to own a ski mask and crowbar and essentially what we would consider break and enter tools, but any police officer would be in the right to arrest someone sitting outside a home at two o'clock in the

Comment s'y prennent-ils généralement aujourd'hui? La façon la plus courante, dont vous avez peut-être entendu parler, c'est le clonage de cartes de crédit grâce aux brèches de sécurité — des brèches subreptices comme saisir les informations échangées dans des cercles ayant des intérêts communs ou les données que les gens affichent sur Internet les concernant. Un exemple typique serait Facebook, site où les gens affichent leurs renseignements personnels dont peuvent se servir les fraudeurs.

L'autre façon, qui devient de plus en plus répandue, c'est de créer des réseaux zombies, c'est-à-dire qu'on infiltre des ordinateurs personnels pour en prendre le contrôle afin de recueillir les données qui s'y trouvent et de les utiliser. Premièrement, le crime organisé se sert de cette méthode pour subtiliser de l'argent. Deuxièmement, on y a recours pour glaner toutes les données personnelles possibles qui se trouvent dans les ordinateurs infectés et qu'on vend sur le marché noir. Tout un secteur d'activité a pris de l'essor dans les entreprises criminelles : on collecte des renseignements personnels çà et là par divers moyens, et on s'en sert par après. Celui qui glane les renseignements n'est pas nécessairement l'utilisateur ultérieur.

Il faut adopter une stratégie à deux volets pour lutter contre ces réseaux criminels : surveiller d'abord les utilisateurs pour ensuite s'attaquer aux glaneurs.

Je suis disposé à répondre aux questions précises que vous voudrez me poser sur les aspects technologiques du vol d'identité.

La présidente : Aucun d'entre nous n'est ingénieur ni expert en technologie de pointe, mais je suis certaine que nous aurons des questions pertinentes à vous poser, monsieur McMahon.

Le sénateur Wallace : Je vous souhaite la bienvenue, monsieur McMahon. Je vous remercie de vos observations. Comme vous le savez, la présente séance de notre comité porte sur le projet de loi S-4. Je ne suis certes pas un expert en technologie d'Internet ni un spécialiste de tous les domaines que vous maîtrisez.

Je commencerai par une question facile, du moins en ce qui me concerne. Compte tenu de votre domaine de spécialisation, des problèmes technologiques, de l'infiltration par le crime organisé et des répercussions de cette infiltration sur le vol d'identité, véritable fléau pour notre société, je me demande ce que vous pensez du projet de loi S-4. D'après vous, de quelle façon permet-il de s'attaquer au problème que nous avons?

M. McMahon : Ayant eu l'occasion d'examiner brièvement le projet de loi et de consulter mes collègues, je pense qu'en adoptant des lois et en ayant la capacité de poursuivre les contrevenants au Canada, une partie du problème est réglée ou atténuée. L'autre partie nécessite une solution technique.

Sans vouloir aborder directement les aspects juridiques de la question, je pense qu'il est important de se doter des outils nécessaires pour demander des comptes aux gens qui ont usurpé un million d'identités ou 10 000 identités à l'aide de leur ordinateur. Il y a manifestement quelque chose qui cloche. J'utilise une analogie pour vous expliquer : il n'est pas illégal de posséder une cagoule de skieur et un pied-de-biche, qui sont essentiellement des outils utilisés pour s'introduire par effraction,

morning dressed in a ski mask and carrying those sorts of things. We need to have legislation that provides analogous powers to be able to prosecute.

It is also a pragmatic question. I think that if someone has on their computer, for example, 10,000 identities, as I understand it the courts must bring in all those individuals and have them testify as to whether they gave that person the right to have their identity on that computer. We need to change that around so that the person who has accumulated all those identities is called to question to justify why he or she has those.

Legislation only works so far as you are prosecuting criminals you can get your hands on within Canada. A great number of the attacks and activity, at least in one part, if not the entire operation, is conducted abroad, as well as where Canadians' information lies. If you have a Hotmail account, Facebook or things like that, the information is not necessarily within Canada.

Senator Wallace: As you point out, each of us at times could be in possession of identity information of someone else, and the issue becomes why you have that and what the purpose of that is. The purpose of Bill S-4 is to deal with identity theft at the stage of that possession or that collection. It is not simply the fact that an individual has that information, but just looking at proposed section 402.2, that the individual possesses another person's identity information in circumstances giving rise to a reasonable inference to commit a crime. There is a requirement that there be this reasonable inference. It is not simply black and white.

Do you feel that this is a significant issue in terms of the technology that you deal with on a day-to-day basis? Is this issue of identity theft a critically important issue that we as parliamentarians should be acting upon immediately, or can it be left for another day?

Mr. McMahon: I think it is an important issue, one that will be emerging as a more critical issue specifically because of the cyber aspect. The easiest form of identity theft is credit card fraud. Credit cards now have smart chips in them, which is now driving a lot of the fraud online, so strong legislation is one part of a solution to going after this sort of thing. Identity theft and cybercrime are becoming extremely profitable on a very large scale.

Senator Wallace: Is that activity under the control of organized crime or has it been infiltrated to a large extent by organized crime?

Mr. McMahon: It used to be, 20 or 10 years ago as the Internet emerged, that you had hackers hacking for the sake of controlling computer systems. Organized crime had not really gone on the Internet and become users of Internet technology. In the last five years, organized crime has essentially taken over nearly everything bad that is happening on the Internet right now. That came about primarily when people were able to make money from the Internet.

mais tout policier aurait le droit d'arrêter quiconque se promènerait ainsi affublé en public en plein cœur de la nuit. Il faut adopter des lois qui donnent le pouvoir d'intenter des poursuites pour vol d'identité.

Il y a également un aspect pragmatique. Si, par exemple, l'inculpé a 10 000 identités dans son ordinateur, je crois comprendre que le tribunal doit faire comparaître ces personnes pour leur demander si elles ont donné à l'inculpé le droit d'avoir leur identité dans son ordinateur. Il faut inverser le fardeau de la preuve, de sorte qu'il incombe à l'inculpé de se justifier.

Une mesure législative n'est efficace que si les criminels visés se trouvent au Canada. Un grand nombre de cyberattaques sont commises en partie sinon en totalité à partir d'un autre pays, et les renseignements personnels sur les Canadiens se trouvent souvent à l'étranger. Si vous possédez un compte avec Hotmail ou Facebook notamment, les renseignements ne se trouvent pas nécessairement au Canada.

Le sénateur Wallace : Comme vous l'avez fait remarquer, nous pouvons tous parfois posséder des renseignements personnels de quelqu'un d'autre. Il s'agit alors de déterminer quels sont nos motifs pour les posséder et à quelles fins on s'en sert. Le projet de loi S-4 porte sur le vol d'identité aux étapes de la possession et de la collecte. Il ne s'agit pas uniquement d'avoir en sa possession des renseignements. Aux termes de l'article 402.2 du projet de loi, commet une infraction quiconque a en sa possession des renseignements identificateurs sur une autre personne dans des circonstances qui permettent de conclure raisonnablement qu'ils seront utilisés dans l'intention de commettre un acte criminel. Il faut pouvoir le conclure raisonnablement. Ce n'est pas une question facile à trancher.

Estimez-vous que ce soit un problème important par rapport à la technologie que vous utilisez quotidiennement? Le vol d'identité est-il un problème crucial auquel les parlementaires que nous sommes devraient s'attaquer immédiatement ou est-ce un problème qui n'est pas urgent?

M. McMahon : C'est, à mon avis, un problème important, qui prendra plus d'ampleur à cause d'Internet. Le clonage de cartes de crédit constitue le vol d'identité le plus facile à commettre. Les cartes de crédit sont désormais dotées de puces savantes, ce qui est à l'origine d'une grande partie des fraudes en direct. Des mesures législatives rigoureuses sont donc une partie de la solution à ce problème. Le vol d'identité et le cybercrime sont devenus extrêmement profitables à une très grande échelle.

Le sénateur Wallace : Le crime organisé contrôle-t-il le vol d'identité ou a-t-il infiltré massivement cette activité?

M. McMahon : Lorsqu'Internet a pris son élan il y a 10 ou 20 ans, les pirates informatiques ne faisaient de l'intrusion que pour contrôler des ordinateurs. Le crime organisé n'avait pas vraiment envahi le créneau d'Internet ni n'utilisait ses technologies. Au cours des cinq dernières années, il est responsable de presque tous les méfaits commis sur Internet, ce qui correspond à l'époque où il est devenu possible de faire de l'argent par le biais d'Internet.

Senator Wallace: As you point out, it is not a problem that exists only within the boundaries of our country or any other; it is an international problem. It is one that requires an immediate approach here in Canada, I believe.

Mr. McMahon: Absolutely.

The Chair: Did I understand you to say that these new credit card chips increase the risk, the likelihood or the number of identity thefts?

Mr. McMahon: No, they shift the vector that the threat agents, like organized crime, are going after. Specifically, if organized crime had a certain amount of time in their day to steal, let us say 50 per cent was spent online and 50 per cent was spent going after credit cards. Now credit and bank cards are becoming much harder. In Europe, they switched over earlier and they noticed a dramatic increase in crime moving online, so we have known for a time. That is where it has shifted right now.

The Chair: Thank you.

Senator Milne: We have heard about the methods of stealing debit and credit card data. We have heard about synthetic identity fraud and we heard last night about theft of courier bags. Now, you have added two more: collecting IDs and using IDs.

I assume Bell is particularly concerned about the collecting of IDs because this happens over the phone lines and over the Internet, whether that on a phone line or not. At Bell, do you have any methods that would help identify when this is happening over your network?

Mr. McMahon: This is a bit of a two-part answer. One, a great many transactions happen every second — a massive number of transactions — as well as malicious activity. There is so much malicious activity that it can be overwhelming. In a traditional sense, let us say you went to the police with a very large fraud, $1-million fraud. You would get their attention and they would start an investigation. On the other hand, suppose you went to the police now and said, "I have $1-million fraud but it is happening in $1 increments, so I have a million $1 frauds." Investigating those requires a completely different set of skills as well as the ability to prosecute.

We are finding that, although anything is technically possible in terms of monitoring threat activities, it is a challenge, and the question is whether you should spend your time chasing down crimes after they have occurred or devote more of your time to proactively trying to prevent these things from happening.

By the way, monitoring is something the financial community does. To a certain extent, telecom organizations monitor the types of threat activity that occur over the network from a technological network basis.

Senator Milne: Are you being proactive in prevention?

Le sénateur Wallace : Vous avez indiqué que ce n'est pas un problème susceptible d'être circonscrit à un pays donné. C'est un problème international, qui ne connaît pas de frontières et auquel il faut s'attaquer immédiatement au Canada, selon moi.

M. McMahon : Tout à fait.

La présidente : Sauf erreur, vous avez dit que les nouvelles puces intégrées aux cartes de crédit chips accroissaient les risques ou les probabilités en ce qui concerne le vol d'identité dont le nombre augmenterait?

M. McMahon : Non, ce qui a changé, c'est le créneau qu'ont investi les agents de menace comme le crime organisé. Je m'explique : le crime organisé s'adonne au vol pendant un certain nombre dans une journée, la moitié de ces heures est utilisée pour les fraudes en direct et l'autre moitié pour le clonage des cartes de crédit. Les cartes de crédit et les cartes bancaires sont de plus en plus difficiles à cloner. En Europe, la transition s'est faite plus tôt, et on a remarqué une augmentation spectaculaire du cybercrime, ce que nous savions depuis un certain temps. C'est ce qui se passe à l'heure actuelle.

La présidente : Merci.

Le sénateur Milne : Nous avons entendu parler des méthodes employées pour voler les données des cartes de débit et de crédit. Nous avons entendu parler de fraude d'identité et, hier soir, de vols de sacs de messageries. Et vous ajoutez deux aspects nouveaux : la collecte de renseignements identificateurs et leur utilisation.

Je suppose que la collecte de renseignements identificateurs inquiète particulièrement Bell parce qu'elle se fait à l'aide des lignes téléphoniques ou d'Internet branché ou non à une ligne téléphonique. Bell emploie-t-elle des méthodes qui permettent de déceler ces intrusions?

M. McMahon : Ma réponse comportera deux volets. Premièrement, beaucoup d'actes malveillants et de transactions sont effectués chaque seconde. On parle d'un nombre faramineux et renversant. Prenons un exemple classique : vous demandez l'aide de la police pour élucider une fraude très importante de un million de dollars. Elle vous prêterait alors une oreille attentive et entreprendrait l'enquête. Par contre, supposons que vous disiez à la police : « Une fraude de un million de dollars a été commise, mais il s'agit d'une fraude de un dollar répétée un million de fois. » Ces deux enquêtes nécessiteraient des compétences complètement différentes et la capacité de poursuivre en justice.

Même s'il est possible de surveiller de telles menaces sur le plan technique, nous constatons que cela pose problème. Il faut également déterminer s'il faut consacrer son temps aux crimes qui ont été commis ou être davantage proactifs dans le domaine de la prévention.

En passant, les établissements financiers s'adonnent à la surveillance. Dans une certaine mesure, les entreprises de télécommunications surveillent les menaces possibles sur leur réseau sur le plan technologique.

Le sénateur Milne : Êtes-vous proactifs en matière de prévention?

Mr. McMahon: Yes. For example, about 94 per cent of email traffic is spam-related and malicious content. Most of that is filtered out before it is passed out to the consumer base. Spam is important because it is one of the means where organized crime, for instance, can get pieces of malicious code into someone's system and be able to steal their identity or take over their system. A proactive means would be stopping that before it happens.

Blacklisting known threat agents or groups and identifying organizations by their IP address and domains are problems. That is acting more proactively in terms of trying to stop that.

That being said, as we know, identity fraud online still persists. Part of the challenge there is balancing a citizen's right to privacy and Net neutrality and how far one goes in policing the content and where people go and what they do online.

Senator Milne: Does Bell ever say to the police, "We know this is happening over our system"?

Mr. McMahon: I think all the carriers, including Bell, have an ongoing dialogue with the police as well as with government and other carries around the world. It is an ongoing, daily dialogue.

There are many challenges in how to tackle the problem, especially given that most of the attacks of this nature are happening from a foreign base of operation.

Senator Milne: Madam Chair, if I ever collected all the multi-millions of dollars I have been offered over the Internet for interceding with someone in Africa with a bank —

The Chair: Just give them your bank account number and the millions will be deposited.

Senator Milne: I hope Bell will be able to do something to stop this. Are you doing anything to stop that kind of spam?

Mr. McMahon: Absolutely. Bell publishes a responsibility report in which we look at the initiatives we take — everything from child safety to "stop spam" initiatives. We sit on all the international committees on spam, as well as taking profound technological measures. We are reducing it significantly, I would say. "Significantly" meaning reducing 90 to 94 per cent of spam that goes to our consumer base.

Senator Bryden: What is there in Bill S-4 that will make the preventative measures you have just been describing more successful?

Mr. McMahon: The bill is obviously intended for a Canadian audience and Canadian perpetrators. The literature tells us a Canadian identity is most usefully exploited within a Canadian context. If someone had my identity, he could probably get the most out of it by trying to use it to open a Canadian bank account

M. McMahon : Oui. Par exemple, environ 94 p. 100 des courriels sont des pourriels ou ont un contenu malveillant. La plupart sont filtrés avant d'être acheminés aux destinataires. Les pourriels ont leur importance parce qu'ils permettent au crime organisé notamment d'introduire un code malveillant dans un ordinateur personnel pour voler des renseignements identificateurs ou contrôler cet ordinateur. Pour être proactifs, il faudrait pouvoir arrêter cela avant qu'il ne se produise.

Établir la liste noire des agents ou des groupes qui présentent une menace et identifier les organisations par leur domaine et leur adresse IP posent problème. Il faut être davantage proactif pour essayer de prévenir cela.

Cela étant dit, la fraude d'identité en direct a toujours cours, comme nous le savons. La difficulté consiste notamment à trouver un compromis entre le droit à la vie privée du citoyen et la neutralité d'Internet ainsi qu'à déterminer le degré de surveillance du contenu et des activités des utilisateurs.

Le sénateur Milne : Bell a-t-elle déjà signalé à la police que des choses suspectes se produisent dans son réseau?

M. McMahon : Je pense que tous les fournisseurs, y compris Bell, collaborent avec les corps policiers et le gouvernement ainsi qu'avec les fournisseurs dans les autres pays. C'est une collaboration constante et quotidienne.

Pour s'attaquer au problème, il faut surmonter beaucoup d'obstacles, compte tenu particulièrement que la plupart des cyberattaques émanent d'un autre pays.

Le sénateur Milne : Madame la présidente, si j'avais touché tous les millions de dollars qu'on m'a promis sur Internet. Il suffisait de communiquer avec quelqu'un en Afrique...

La présidente : Il suffit de donner son n° de compte bancaire pour que les millions soient déposés.

Le sénateur Milne : J'espère que Bell sera en mesure d'enrayer cela. Prenez-vous des mesures pour mettre un terme à ce genre de pourriels?

M. McMahon : Tout à fait. Bell publie un rapport sur la responsabilité d'entreprise, dans lequel nous examinons les mesures que nous prenons : de la sécurité des enfants jusqu'à la lutte contre les pourriels. Nous siégeons à des comités internationaux qui se penchent sur les pourriels et nous adoptons des mesures technologiques exhaustives. Je dirais que nous réduisons le nombre de pourriels considérablement. Par « considérablement », j'entends de 90 à 94 p. 100 des pourriels que nous recevons.

Le sénateur Bryden : En quoi le projet de loi S-4 rendra-t-il plus efficaces les mesures de prévention que vous venez de décrire?

M. McMahon : Le projet de loi vise de toute évidence le public canadien et les auteurs d'infraction canadiens. D'après les documents que nous avons consultés, l'identité canadienne est plus facilement exploitable au Canada. Si quelqu'un avait usurpé mon identité, il pourrait probablement en faire la meilleure

and buy Canadian goods, rather than trying to use my account and identity in Thailand, for example.

When it comes to protecting Canadians, part of the solution — though not the whole solution — will reside within Canada. To that extent, I think the bill is extremely useful in allowing prosecutors to take down the people we can actually reach out and touch.

There are other ways and means we can look at for working collaboratively with the United States and other partners to put down identity theft around the world.

Senator Bryden: Within Canada, specifically, what is in this bill that makes it easier to catch the Canadian people who are doing that versus what is available to you now?

Mr. McMahon: I am speaking from a technological basis. From what I understand from talking with my legal colleagues, this bill goes one step further down the road to helping them prosecute cases involving identity theft, or at least raising it up to the consciousness.

Part of the challenge is always how you map the technological modus operandi that someone has used with the letter of the law. I think I am probably out of my range talking about that.

Senator Bryden: I have one small point. It was mentioned yesterday that the types of offences described in Bill S-4 are at the lower end of the seriousness level. That is one of the reasons the penalties are not very high. Maximums are basically $5,000.

It is a problem with police in other areas that if the potential penalties are very low, like the penalties listed in Bill S-4, and the police are busy, they simply do not or will not take the time to go after those activities. It is simply not worth the policeman's time when there are many more rewarding things for a professional police force to deal with and much demand.

Will that be a problem? Do you have difficulty in having police trace down these users of other people's identities on a regular basis currently?

Mr. McMahon: The inherent challenge is that tools, methods, techniques and modus operandi change very rapidly. There are technological ways to perpetrate crime on the Internet that we are not sure there are laws to cover or, at least, legal interpretation to circumvent.

Another challenge is that instead of big heists, we are talking about millions of small heists and a widely distributed criminal network. It is easier, relatively speaking, if you have one criminal with one large heist within Canada. You can take that person down. If you have many people involved in tens of thousands or millions of small heists where none of the victims realize that they were victims and are not coming forward to the police, that becomes a big challenge, especially when no one has reported it to police. It exists on the Internet and you may get some insight into it.

utilisation possible en ouvrant un compte dans une banque canadienne et en achetant des produits canadiens au lieu de s'en servir en Thaïlande, notamment.

Lorsqu'il s'agit de protéger les Canadiens, une partie de la solution — pas toute la solution cependant — consiste à intervenir au Canada. C'est pourquoi j'estime que le projet de loi est extrêmement utile en permettant de poursuivre ceux sur qui on peut mettre véritablement la main.

On peut envisager d'autres moyens afin de collaborer avec les États-Unis et d'autres pays en vue de mettre un terme au vol d'identité dans le monde.

Le sénateur Bryden : Plus particulièrement, dans quelle mesure le projet de loi permet-il plus facilement de mettre la main sur les Canadiens que les moyens dont vous disposez actuellement?

M. McMahon : Je répondrai sur le plan technologique. Selon mes collègues du domaine juridique à qui j'en ai parlé, le projet de loi permettra davantage d'intenter des poursuites dans le cas de vol d'identité ou à tout le moins de sensibiliser davantage les gens à cette question.

Il faut toujours établir si le mode de fonctionnement technologique utilisé est visé par l'esprit de la loi. C'est une partie du problème. Je pense que cette question ne relève pas de mon domaine de compétence.

Le sénateur Bryden : Je voudrais obtenir une petite précision. On a indiqué hier que les infractions figurant dans le projet de loi S-4 sont parmi les moins graves. C'est pourquoi notamment les pénalités ne sont pas très élevées. Le maximum est de 5 000 $.

Les pénalités très peu élevées comme celles du projet de loi S-4 posent également un problème aux policiers dans d'autres domaines. Ceux-ci sont occupés, et ils n'ont pas ou n'auront pas le temps de s'attaquer à ce genre d'activités alors qu'ils sont confrontés à des problèmes beaucoup plus pressants et exigeants.

Y voyez-vous là un problème? À l'heure actuelle, avez-vous de la difficulté à obtenir la collaboration régulière des corps policiers pour enquêter sur les vols d'identité?

M. McMahon : Le problème, c'est que les outils, les méthodes, les techniques et le modus operandi changent très rapidement. Il existe des moyens technologiques de commettre des crimes sur l'Internet qui ne sont peut-être pas visés par des lois ou, du moins, des lois dont l'interprétation permettrait de les mettre en échec.

L'autre problème, c'est qu'il est question de millions de petits larcins, plutôt que de grands crimes, et d'un réseau de criminels très étendu. Il est relativement plus facile d'épingler le criminel qui commet un grand vol au Canada même. Il est possible de le prendre. Par contre, quand de nombreuses personnes commettent des dizaines de milliers ou des millions de petits vols et que les victimes ne sont même pas conscientes qu'elles le sont de sorte qu'elles ne les signalent pas à la police, le problème est encore plus grand, surtout s'il n'y a pas de signalement. C'est un problème présent sur l'Internet, et vous arriverez peut-être à le cerner jusqu'à un certain point.

This type of crime requires non-traditional policing covered by non-traditional legislation. Some creativity in how prosecutors will interpret the law and police will eventually be able to enforce it is needed. It definitely will rely on cooperation of different communities of interest, such as the financial community, Internet service providers, carriers, and the retail industry to provide that operational situational awareness for the police as to where to start looking.

Senator Joyal: I will wait my turn since the explanation given by the witness is covering elements that I wanted to raise.

Senator Baker: The Personal Information Protection and Electronic Documents Act, PIPEDA, that we passed in Parliament recently, apart from the Privacy Act, applies to telephone companies because they are a federal work under the act. That came into effect in January 2001. I have noticed several judgments involving Bell and other telephone companies. Yesterday Senator Nolin brought to our attention a provision in Bill S-4 involving the rights and the extent of those rights given to police officers in that they are excluded from certain sections of this act.

As I recall, the Privacy Act and PIPEDA also have exceptions regarding police investigations. If you were telephoned by some police force from a small community anywhere to give them privacy information, would that normally be restricted under the legislation?

Mr. McMahon: Yes, senator. There are clear black and white areas that are very easy to determine. For example, one black and white area is where a law enforcement agency wants to put up a wiretap. It requires a federal warrant.

Senator Baker: That is a warrant. I am not talking about warrants.

Mr. McMahon: Yes, exactly. That is one side that is very clear. The other side would be when a police force wants a general picture on the nature of cybercrime. That is a professional consulting engagement.

It is the items in the middle where we have the privacy debate, security discussions and things like this. Almost all times it can be resolved one way or the other and people and law enforcement can get what they need.

Some of the challenges are pragmatic. It depends on how much information the police need and whether they have a priori the information we require in order to go look for more information, or whether the questions are too vague and require more investigative support. For example, child safety issues and online exploitation of children are usually dealt with very cleanly. If the question is vaguer and it becomes a fishing

Ce genre de crime exige des méthodes policières inédites prévues dans des lois nouvelles. Il faudra que les procureurs fassent preuve d'un peu d'imagination dans la manière dont ils interpréteront la loi et la police, dans sa façon de l'appliquer. Ces lois reposeront certainement sur la coopération entre les intéressés, par exemple le milieu financier, les fournisseurs d'Internet, les entreprises de télécommunication et l'industrie du commerce au détail, de manière à pouvoir fournir à la police un certain contexte opérationnel qui lui permettra de dégager des pistes d'enquête.

Le sénateur Joyal : Je vais attendre mon tour puisque les explications fournies par le témoin ont répondu à certaines de mes questions.

Le sénateur Baker : La Loi sur la protection des renseignements personnels et les documents électroniques que le Parlement a adoptée récemment, isolément de la Loi sur la protection des renseignements personnels, s'applique aux entreprises de téléphonie parce qu'elles sont réputées être de compétence fédérale. Cette loi est entrée en vigueur en janvier 2001. J'ai remarqué plusieurs décisions rendues qui mettent en cause Bell et d'autres entreprises de téléphonie. Hier, le sénateur Nolin a attiré notre attention sur une disposition du projet de loi S-4 relative aux droits et à la portée des droits conférés aux policiers, en ce sens qu'ils sont exclus de certains articles de la loi.

Si je ne m'abuse, la Loi sur la protection des renseignements personnels et la Loi sur la protection des renseignements personnels et les documents électroniques prévoient également des exceptions dans le cas d'enquêtes policières. Si vous receviez l'appel du policier d'une petite localité qui vous demandait de lui fournir des renseignements personnels, la loi limiterait-elle les renseignements que vous pouvez communiquer habituellement?

M. McMahon : Oui, sénateur. Il existe des zones bien définies qui sont faciles à comprendre. Par exemple, si un organisme d'application de la loi souhaite faire de l'écoute électronique, il faut qu'il obtienne d'abord un mandat fédéral.

Le sénateur Baker : Vous parlez de mandat, mais ce n'est pas ce dont je parle.

M. McMahon : Justement. C'est là un aspect de la loi qui est très clair. Par contre, là où elle l'est moins, c'est lorsqu'une force policière demande à obtenir un tableau général illustrant la nature du cybercrime. Il s'agit alors d'une consultation professionnelle.

Ils existent une foule d'autres cas moins tranchés qui suscitent un débat sur la protection de la vie privée, sur la sécurité et ce genre de choses. Presque toujours, on arrive à une solution quelconque et à obtenir ce dont on a besoin.

Certains des problèmes sont d'ordre pragmatique. Tout dépend de la quantité d'information dont a besoin la police et du fait qu'elle dispose à priori de l'information dont nous avons besoin pour nous permettre d'aller en chercher plus ou le fait que la question soit trop vague et exige plus de soutien à l'enquête. Ainsi, il est habituellement très facile de régler les questions relatives à la sécurité et l'exploitation en ligne des enfants. Si la question est

expedition, then we would have questions. We would be balancing the privacy of our clients and subscriber databases with the needs of law enforcement.

Senator Baker: You have within the cellular and land line operations a special office that deals with law enforcement.

Mr. McMahon: Yes, absolutely.

Senator Baker: In other words, when the police come to you with a number recorder warrant under section 492.2 of the Criminal Code, you have that person in that office deal with the police. That is a warrant to get telephone numbers.

Mr. McMahon: Yes.

Senator Baker: That office would also deal with a warrant when you want to tap someone's telephone.

However, I am particularly interested in this act as it relates to that person or persons in those offices talking on the telephone to police and giving out persons' addresses, unlisted telephone numbers, and other information. This appears to be a practice with all telephone companies. Is this because you interpret that PIPEDA does not to apply in the case of police officers asking for information? Do you have any thoughts on that?

Mr. McMahon: How much information you would provide in the absence of a very specific warrant would depend on the circumstance and the urgency of the case.

Senator Baker: I am not talking about a warrant. I am talking about information given voluntarily by telephone companies to anyone who phones, specifically a police officer.

Suppose they are using a "swamper" that collects cellular telephone numbers in a specific area. Police telephone your office to set up to deal with them and ask for the name, address and all of the information you have concerning that number. It is given without warrant. I am wondering how that takes place without judicial authorization.

Mr. McMahon: Typically we would have a warrant to provide that sort of information.

Senator Baker: Are you saying it does not happen?

Mr. McMahon: Not from my office. However, I do not deal specifically with that or identity theft.

The Chair: Senator, may I put you down for a second round?

Senator Baker: I have one more question relating to another subject.

The Chair: It will come on a brilliant second round.

plus floue et se transforme en expédition de pêche, alors nous posons des questions. Il nous faut frapper un juste équilibre entre la protection de la vie privée de nos clients et de nos fichiers sur les abonnés et les exigences d'application de la loi.

Le sénateur Baker : Vous avez, dans votre secteur de téléphonie cellulaire et de lignes terrestres, un bureau spécial qui s'occupe de l'application de la loi.

M. McMahon : Oui.

Le sénateur Baker : En d'autres mots, lorsque la police se présente avec un mandat l'autorisant à placer un téléphone sous enregistreur de n^{o} en vertu de l'article 492.2 du Code criminel, c'est la personne qui travaille dans ce bureau qui traite avec elle. Il s'agit là d'un mandat visant à obtenir des n^{o}s de téléphone.

M. McMahon : Oui.

Le sénateur Baker : Ce serait aussi ce bureau qui s'occuperait d'un mandat d'écoute téléphonique.

Toutefois, je m'intéresse particulièrement aux aspects de la loi mettant en cause cette personne qui parle aux policiers au téléphone et leur fournit des adresses, des n^{o}s de téléphone non inscrits et ainsi de suite. La pratique semble répandue au sein de toutes les entreprises de téléphonie. Est-ce parce que, selon votre interprétation, la Loi sur la protection des renseignements personnels et les documents électroniques ne s'applique pas lorsque des policiers demandent de l'information? Avez-vous une opinion à ce sujet?

M. McMahon : La quantité d'information fournie en l'absence d'un mandat très précis serait fonction des circonstances et de l'urgence de la demande.

Le sénateur Baker : Je ne parle pas de mandat. Je parle de renseignements fournis volontairement par les entreprises de téléphonie à quiconque appelle, plus particulièrement un policier.

Prenons l'exemple du dispositif qui permet de connaître tous les n^{o}s de téléphone cellulaire dans un secteur particulier. La police appelle à votre bureau pour organiser une rencontre afin de connaître le nom, l'adresse et toute l'information détenue au sujet d'un certain n^{o}. L'information est fournie sans mandat. Je me demande comment il est possible d'accéder à une pareille demande, sans l'autorisation d'un juge.

M. McMahon : Typiquement, il faudrait qu'il y ait un mandat nous autorisant à communiquer ce genre de renseignements.

Le sénateur Baker : Êtes-vous en train d'affirmer que cela ne se produit jamais?

M. McMahon : Pas chez nous. Toutefois, je ne m'occupe pas particulièrement de ce genre de demandes ou de vol d'identité.

La présidente : Sénateur, puis-je inscrire votre nom sur la liste des intervenants pour le second tour de table?

Le sénateur Baker : J'ai une autre question à poser concernant un tout autre sujet.

La présidente : Vous pourrez la poser lors du génial second tour de table.

Senator Joyal: Mr. McMahon, you mentioned in your presentation that the technology is moving fast. How much of an element of flexibility to adapt to new technology should we try to bring into this legislation, so that it is not obsolete in two or five years down the road? I ask because the system will have been refined by then and become more sophisticated, and it will be easier for hackers to move into it and steal the credit card numbers or someone's identity.

You have read the legislation, I am sure. Is there an element in it that you would suggest to us to think twice about and ensure we are able to be responsive, either in the definitions or in the other aspects — the way the offences are defined?

Mr. McMahon: I went through a similar exercise a number of years ago looking at wiretap laws and other types of legislation in the Criminal Code that had a technology bias to them.

The best advice I had for myself at the time was to try to keep the legislation open enough and not nail it down to specific technologies, means, modes or methods because those evolve so rapidly. That gives the prosecutors or the legal community the ability to rationally interpret the laws to the evolving technology. That is the first part of the answer.

The other part of the answer is that there are things that need to occur outside the technology in order to help us deal with identity theft. Those are about developing countermeasures to identity theft and include everything from security awareness campaigns for the public and disclosure. It also includes various public-private partnerships in developing technologies that would provide a safer online environment.

There are many different things. The legislation is one part of it, of course.

Senator Joyal: How much are you involved in the responsibility to develop, as you said, counter-approaches to the ones the offender would like to have in order to protect the public?

I have a concern and I will give you an example. When we around this table were concerned about child pornography, a responsibility was put on Internet service providers. Could we make a similar or analogous reasoning stating that we know that there is a break and entry in the system and, as a provider of that service, you, to a point, have a responsibility to make it tight?

In this bill, should there be anything analogous to the one we did for child pornography? Or should we not spell out a responsibility for the provider of those services. Did you pay any attention to that in the past?

Le sénateur Joyal : Monsieur McMahon, vous avez mentionné dans votre déclaration que la technologie évolue rapidement. À quel point faut-il rendre le projet de loi adaptable aux nouvelles technologies, pour éviter que la loi ne soit désuète dans deux ou cinq ans? Je vous pose la question parce que le réseau aura peaufiné ses façons de faire d'ici là et se sera perfectionné, de sorte qu'il sera plus facile aux pirates informatiques d'y entrer illégalement pour voler des n^{o}s de carte de crédit ou des identités.

Vous avez, j'en suis sûr, lu le projet de loi. Y a-t-il un élément dans le texte auquel il faudrait, selon vous, réfléchir davantage et faire en sorte qu'il soit possible de l'adapter, soit dans les définitions ou ailleurs — la manière dont les infractions sont définies?

M. McMahon : On m'a posé la même question il y a quelques années au sujet des lois sur les tables d'écoute et d'autres genres de mesures prévues dans le Code criminel qui visaient la technologie.

Le meilleur conseil que je pouvais donner alors était d'essayer de laisser la porte suffisamment grande ouverte et de ne pas viser des technologies, des moyens, des modes ou des méthodes particuliers en raison de leur évolution rapide. Ainsi, les procureurs ou les avocats pourront interpréter la loi de manière rationnelle, en fonction de l'évolution de la technologie. C'est là la première partie de la solution.

L'autre, c'est qu'il existe d'autres mesures à prendre, à l'extérieur du domaine technologique, pour aider à contrer le vol d'identité. Il faudra notamment développer des contre-mesures au vol d'identité et tout inclure, des campagnes de sensibilisation à la sécurité destinées au grand public à la communication de renseignements, y compris divers partenariats publics-privés visant à développer des technologies qui offriront un environnement en ligne plus sécuritaire.

Il y a de nombreuses choses à faire. La loi ne représente qu'une partie d'entre elles, naturellement.

Le sénateur Joyal : À quel point participez-vous à la responsabilité d'élaborer, comme vous l'avez dit, des contre-mesures visant à protéger le grand public?

Une chose me préoccupe, et je vous en donne un exemple précis. Les membres du comité, préoccupés par la pornographie juvénile, ont recommandé de confier une responsabilité aux fournisseurs d'accès Internet. Pourrions-nous tenir le même raisonnement ou un raisonnement analogue et dire que nous savons qu'il y a eu accès illégal au système et qu'en tant que fournisseur d'accès, vous avez jusqu'à un certain point la responsabilité de le rendre impénétrable?

Faudra-t-il, dans le projet de loi à l'étude, inclure quelque chose d'analogue à ce que nous avons fait dans celui sur la pornographie juvénile? Ou serait-il préférable de ne pas conférer de responsabilité au fournisseur d'accès? Y avez-vous déjà réfléchi?

Mr. McMahon: Child safety is a good example. We block explicit child pornography from the Internet to the best of our ability. Right now, we are using a list provided by Cybertip.ca, and that has been a fairly successful program.

The way that providers and carriers around the world handle the threat is very much like a large ecosystem with predators. Our response to predators is to essentially balance itself out. It balances itself out so all the carriers put security mechanisms in place to reduce the amount of online fraud, the theft of bandwidth, the amount of spam and things like that.

It will come to a point where it becomes difficult to clean the pipes any further. Right now, that is around 94 per cent. There are a number of reasons behind that. There are fiscal reasons. It becomes cost-preclusive at a certain point; you get logged in diminishing returns in the security mechanisms you put in. It also gets harder to get the last few per cent. The other one is the lack of clients asking for it, especially because most of them do not know they are victims. Therefore, there are market forces that balance it out, as well.

Net neutrality and privacy issues also come into play. People want to be able to go places, download things, visit sites and so on. There is a limit to what restrictive security policies any carrier can uniformly put on the Canadian public. A bank, for instance, may have very stringent policies that we can put in place, and their networks can be a lot cleaner. The same goes for any particular enterprise. However, when you are providing bandwidth for the general public, you are riding a fine line as to how much security you provide without impinging upon people's privacy issues and providing their ability to operate on the Internet, and get themselves infected in a lot of cases.

That is an ongoing discussion now. Legislation is probably not the answer to moving that bar. We had put forward a proposal for tax credits where we could accelerate programs to provide cleaner pipes, as opposed to trying to create programs and then find a client to help pay for those.

A lot of stuff has been happening, obviously. I think it has been accelerating because of the cost of bandwidth, as well as providing value-added services in providing cleaner pipes and more trustworthy connectivity for clients.

Senator Joyal: In relation to the first question, are there any clauses of the bill where you feel the technology terminology is too limited and not open enough to allow for further interpretation that would adapt to new developments?

Mr. McMahon: I do not think so. I think it would be limited more by the creativity and how much risk a prosecutor is willing to take in interpreting technology — our ability to articulate what

M. McMahon : La sécurité des enfants est un bon exemple. Nous faisons de notre mieux pour bloquer la pornographie juvénile explicite sur l'Internet. Actuellement, nous avons recours à une liste fournie par Cybertip.ca, un programme plutôt bien réussi.

La façon dont les fournisseurs et les entreprises de télécommunication du monde entier font face à la menace évoque l'image d'un énorme écosystème dans lequel il y a des prédateurs. Notre réaction aux prédateurs consiste essentiellement à les neutraliser. Nous neutralisons, de sorte que toutes les entreprises de télécommunication insèrent des mécanismes de sécurité visant à réduire la quantité de fraudes en ligne, de vols de bandes de fréquence, de pourriels et d'autres phénomènes de ce genre.

Le jour viendra où il sera difficile de purger le système davantage. Actuellement, nous bloquons 94 p. 100 environ de ces phénomènes. Il existe plusieurs explications, y compris de nature budgétaire. À un certain stade, le coût devient prohibitif. Les rendements des mécanismes de sécurité mis en place diminuent. Il devient aussi plus difficile de bloquer les quelques pourcents qui restent. Autre raison, peu de clients les demandent, en raison surtout du fait que la plupart d'entre eux ne savent pas qu'ils sont menacés. Par conséquent, les forces du marché sont aussi un facteur déterminant.

Les questions de neutralité nette et de protection de la vie privée entrent aussi en jeu. Les gens souhaitent pouvoir visiter des sites, télécharger, et ainsi de suite. Il y a une limite aux politiques de sécurité restrictives qu'une entreprise de télécommunication peut mettre en place uniformément et appliquer à tout le grand public canadien. Par exemple, il est possible qu'une banque ait des politiques très rigoureuses que nous pouvons mettre en place, de sorte que ses réseaux sont beaucoup plus sécuritaires. Il en va de même pour l'entreprise particulière. Cependant, quand on fournit des largeurs de bande au grand public, il est difficile de fournir de la sécurité sans empiéter sur le droit à la protection de la vie privée des gens et les empêcher de naviguer sur l'Internet et bien souvent de contracter des virus.

Ce débat est en cours. La législation n'est probablement pas la réponse. Nous avions proposé des crédits d'impôt qui nous permettraient d'accélérer les programmes afin d'épurer davantage les systèmes, plutôt que d'essayer de créer des programmes et de trouver des clients pour aider à les financer.

Il y a eu beaucoup d'avancées, de toute évidence. Le phénomène s'accélère en raison du coût de la largeur de bande, ainsi que de la volonté d'offrir aux clients des services à valeur ajoutée, c'est-à-dire des systèmes plus nets et une connectivité plus fiable.

Le sénateur Joyal : En ce qui concerne la première question, y a-t-il dans le projet de loi des passages où les termes techniques ont un sens trop restrictif qui empêchera une adaptation aux nouvelles avancées?

M. McMahon : Je ne le crois pas. Je crois que la loi serait davantage limitée par la créativité et par la part de risque que le procureur est disposé à assumer dans l'interprétation de la

is happening in real time in cyberspace, from a threat perspective, to people with a legal background that can make that interpretation.

Senator Joyal: Do you feel that all the areas of biometrics that we are talking about are spelled out in sufficiently general terms to allow the bill to be effective years down the road, with all the development that we can expect in relation to that technology?

Mr. McMahon: I think so. I have not looked at the bill with that perspective. Again, I would only caution against becoming too technical in a bill because, as soon as you put in a technical solution, you are likely to be outdated within months — six months to a year.

The Chair: I want to explain that it is not from lack of interest that I keep moving people along. It is just that we do face time constraints and everybody wants to get a chance to put questions to you, Mr. McMahon. That is our difficulty.

Senator Nolin: My question is more of a curiosity because you are here representing the Information Technology Association of Canada. I am sure among your membership, you may have the answer.

Most of us travel and hotel rooms open with a card. We have been told to watch out for those cards, that they may contain information that could be used against us. Is that true, and how does it work? I cherish that card. I keep it in my drawer in my office just to ensure nobody will see it. What is in there? Is my credit card number on it? What is on that card that I should protect?

Mr. McMahon: What is the card you are referring to?

Senator Nolin: The card that opens your hotel door. Are you familiar with that technology? Is it just a signal that opens the door?

Mr. McMahon: It is a difficult question to answer because there are so many different card technologies involved.

Senator Nolin: That is why I do not know the answer.

Mr. McMahon: Very simply, certain cards will contain more information on you than others. It is really up to the discretion of the people building and using the cards as to what to put on. There are several basic cards. I put them in two or three categories: one is a card with a magnetic strip that you can put anything you want on; another has some sort of chip technology that encrypts the information and allows a more secure exchange of information.

More and more, we are moving to cards of interest, like bank cards and credit cards, using chip technology, which has now placed the work factor for prosecuting and attacking those cards into an area where it is more difficult to deal with those than it is to do things other ways. With just a plain card with no chip, the

technologie — notre capacité d'énoncer ce qui se passe en temps réel dans le cyberespace, du point de vue des menaces, à des gens ayant des connaissances juridiques capables d'en faire l'interprétation.

Le sénateur Joyal : Estimez-vous que tous les domaines biométriques dont nous parlions sont décrits en termes suffisamment généraux pour permettre au projet de loi de conserver son actualité pendant plusieurs années, étant donné tous les développements de la technologie auxquels on peut s'attendre?

M. McMahon : Je le crois. Je n'ai pas examiné le projet de loi sous cet angle. À nouveau, je ne puis que vous mettre en garde contre la tentation de trop verser dans les détails techniques parce que, si vous prévoyez une solution technique, elle sera probablement désuète dans quelques mois, dans six mois ou un an.

La présidente : Je tiens à préciser que ce n'est pas par manque d'intérêt que je cède la parole à d'autres. Par contre, nous devons respecter des limites de temps et tous tiennent à pouvoir vous poser des questions, monsieur McMahon. C'est là le problème.

Le sénateur Nolin : Ma question relève davantage de la curiosité parce que vous êtes ici comme porte-parole de l'Association canadienne de la technologie de l'information. Je suis convaincu que, parmi vos membres, certains ont peut-être la réponse.

La plupart d'entre nous voyagent, et on ouvre la porte des chambres d'hôtel au moyen d'une carte. Nous avons été prévenus de prendre le plus grand soin de ces cartes, qu'elles contiennent peut-être de l'information qui pourrait être utilisée contre nous. Est-ce vrai et, dans l'affirmative, comment cela fonctionne-t-il? J'adore ma carte. Je la garde dans le tiroir de mon pupitre juste pour la mettre à l'abri des regards. Que contient-elle? Mon n^{o} de carte de crédit y figure-t-il? Quels renseignements cette carte comporte-t-elle que je devrais protéger?

M. McMahon : De quelle carte parlez-vous?

Le sénateur Nolin : De la carte qui vous ouvre la porte de votre Chambre d'hôtel. Connaissez-vous la technologie? Transmet-elle simplement un signal qui déverrouille la porte?

M. McMahon : Il m'est difficile d'y répondre parce qu'il existe tant de technologies différentes.

Le sénateur Nolin : C'est pourquoi j'ignore la réponse.

M. McMahon : Pour vous répondre très simplement, certaines cartes renferment plus d'information sur vous que d'autres. Le contenu est en réalité laissé à la discrétion de ceux qui les conçoivent et les utilisent. Il existe plusieurs cartes de base. Je les classe dans deux catégories : la carte à bande magnétique, dans laquelle vous pouvez inclure tous les renseignements désirés, et la carte à puce, qui code l'information et en permet un échange plus sécuritaire.

De plus en plus, nous observons une croissance de l'intérêt marqué à certaines cartes, par exemple les cartes bancaires et les cartes de crédit auxquelles une puce est intégrée. Elles compliquent le travail de la poursuite. Il est plus difficile de traiter ce genre de crimes que les autres. La personne malveillante

challenge is whether it is worthwhile for any particular threat agent to skim those cards in the presence of other means of making money in the time available. The problem criminals have now is an embarrassment of riches.

Senator Nolin: Should I keep storing those cards and not giving them back to the hotel clerk?

Senator Campbell: That is only with keys.

Senator Nolin: Try to find one that uses a key.

Mr. McMahon: I do not know without looking at the specific information they stored on the card.

Senator Nolin: My other question refers to the exchange of information. Within your association, I see an important group of corporations. Do you exchange data? At Bell Canada, do you have a list of information that you are asked to share with others in your association? Do you have a list of names and addresses of people who are breaching the use of Bell Canada services, and are you asked to share that information with other members of your association?

Mr. McMahon: The simple answer is that we do not share any subscriber information with anyone without legal authority. Even if we wanted to, the quantity of information of malicious activity occurring in cyberspace in Canada is so massive that they would not have an Internet pipe big enough or computers large enough to store it. We do typically share summarized reporting regarding the trends of the modus operandi, latest trade craft, the types of things you would see on a Symantec report, taking a vast amount of information and boiling it down to an executive summary of the general themes.

Specific information as to who is doing what to whom is the sort of thing we would discuss with law enforcement, and even then we are both of us moving together in this environment where we have a lot of information but it is just not practical or correct to hand it all over. Now it is mostly exchanged verbally or in reports.

Senator Nolin: Yesterday we asked the Department of Justice whether there was an intent to create a data bank to be shared by the law enforcement organizations across the country, and the answer is no, but I was wondering whether technology could help on that. Obviously not. What you are sharing amongst your membership is trends and techniques used to breach your systems.

Mr. McMahon: Yes. The challenge we have is that the pace and magnitude of the things going on are so great that the analysis must occur within those communities that have access to that primary data. If you are in a financial environment looking at the financial fraud metric, you see that those activities are happening very fast, and it is the same in the telecommunications environment. If you can imagine, these are very large pipes and

va se demander s'il est rentable de voler une simple carte sans puce quand il existe d'autres moyens plus rapides de faire de l'argent. Le problème des criminels actuellement, c'est qu'ils ont l'embarras du choix.

Le sénateur Nolin : Devrais-je continuer de conserver ces cartes et de ne pas les rendre à la réception de l'hôtel?

Le sénateur Campbell : On ne le fait que pour les clés.

Le sénateur Nolin : Y a-t-il encore des hôtels qui utilisent des clés?

M. McMahon : Je ne saurais quoi vous répondre si je ne connais pas l'information précise qui est emmagasinée sur la carte.

Le sénateur Nolin : Mon autre question porte sur l'échange de renseignements. Au sein de votre association, je constate la présence d'un groupe important de sociétés. Partagez-vous des données? À Bell Canada, avez-vous une liste de renseignements que vous êtes priés de partager avec d'autres membres de l'association? Avez-vous une liste de noms et d'adresses de personnes qui ne respectent pas les règles d'utilisation des services de Bell Canada et vous demande-t-on de partager ces renseignements avec d'autres membres de votre association?

M. McMahon : Nous ne partageons pas d'information sur les abonnés avec qui que ce soit sans en avoir l'autorisation légale. Même si nous le voulions, la quantité d'information sur l'activité malveillante qui se déroule dans le cyberespace canadien est si volumineuse qu'il n'y a pas de service Internet ou d'ordinateur suffisamment puissant pour l'emmagasiner. Nous partageons effectivement, habituellement, des rapports qui résument les tendances relatives aux façons de faire, les plus récentes nouveautés dans le métier, le genre de choses que vous liriez dans un rapport de Symantec, soit une grande quantité d'information résumée pour la haute direction sous forme de grands thèmes.

Les renseignements précis sur qui fait quoi à qui représentent le genre de choses dont nous ne discutons qu'avec les organes d'exécution de la loi, et encore là, nous évoluons tous deux dans un environnement où nous avons beaucoup d'information, mais qu'elle n'est tout simplement pas pratique ou suffisamment exacte pour être communiquée. Actuellement, la plupart des échanges d'information se font de vive voix ou au moyen de rapports.

Le sénateur Nolin : Hier, nous avons demandé au ministère de la Justice s'il avait l'intention de créer une banque de données à l'usage de tous les organismes d'application de la loi au pays. Il nous a répondu par la négative. Je me demandais simplement si la technologie pouvait nous venir en aide, mais il semble que non. Ce que vous communiquez à vos membres, ce sont les tendances ainsi que les techniques d'intrusion.

M. McMahon : C'est exact. Le défi, c'est que les techniques se développent et se répandent si vite qu'il faut effectuer l'analyse au sein même des collectivités qui ont accès à ces données brutes. L'analyste du milieu financier qui examine les mesures de la fraude financière constate qu'elle se fait en un clin d'oeil. On observe le même phénomène dans le milieu des télécommunications. Vous pouvez vous imaginer l'étendue des canaux de communication et

very large systems. There is no easy way of boiling that down and summarizing it in real time for people. It takes many people and a fair bit of time to massage it and produce a report and provide that information, which we do regularly.

Senator Nolin: I understand that Bill S-4 will help you in doing your job.

Mr. McMahon: It certainly does not hurt.

Senator Dickson: I would like to preface my question or my remarks with two statements: one, I am a victim of credit card fraud, which I can explain quickly; and two, my daughter works at Bell Canada. I should declare my interest right off. I should have done that first.

The background is that all of a sudden I get a credit card statement, and there I am debited $8,700. What do I do? I go to the bank, rather upset, and explain that I am down $8,700. That is quite a party. I knew I did not incur that. The bank said that the first step was to go to the local detachment of the RCMP or the police. I will not comment on the local police, but the RCMP were very accessible and available, so I reported it there. I called the credit card company back and told them I filed the report, and luckily I got the credit on the card, so I was not responsible for the debt. The bank in turn found the branch through some mechanism in their system — it was a branch in Edmonton — and the identification of a person to whose account the money was transferred from my account.

I understand from the clerk of the committee that credit card companies and probably banks will be invited here, but from the associations that you deal with, there must be codes of practice where you cooperate with the banks and the credit card companies, as well in relation to online banking. Are there effective, technical mechanisms, or could there be better mechanisms in place there?

Mr. McMahon: Yes, there are, senator. The telecommunication companies and the banks work together very closely. They share a partner relationship as well as a client relationship. We tend to manage their networks. We also are implicated or involved in being victimized ourselves. Most of the attacks on the financial industry or their clients and most of those online attacks are perpetrated through the infrastructures that we manage, so we have shared interests, absolutely. We do meet. We do talk. We do exchange information, in some cases, real time.

In trying to track down things like identity fraud, there are two lines of investigation. One is to follow the money, and the other is to follow the communication. You have an IP address, an Internet protocol address or domain name associated with someone who is doing things on line. You may have a financial tracking of the information of where it goes. Those systems are not necessarily integrated. That interface is occurring almost face to face. There may be a time in the future where we can do online correlation to figure out where something has gone off the Internet and where that money trail is happening.

des systèmes. Il n'est pas si facile de résumer l'information en temps réel. L'analyse des renseignements, la rédaction d'un rapport et la communication de l'information que nous faisons sur une base régulière exigent beaucoup de personnel et de temps.

Le sénateur Nolin : Le projet de loi S-4 vous facilitera sûrement la tâche.

M. McMahon : Il ne nuira pas, c'est certain.

Le sénateur Dickson : En avant-propos, je tiens à faire deux déclarations : premièrement, j'ai été victime d'une fraude par carte de crédit, que je peux vous décrire rapidement et, deuxièmement, ma fille travaille chez Bell Canada. Mieux vaut le dire au départ, et j'aurais dû le faire plus tôt.

Je vous explique ce qui s'est passé. Lorsque j'ai reçu le relevé de ma carte de crédit, je me suis rendu compte qu'on avait débité mon compte de 8 700 $. Que faire? Je me rends donc à la banque, plutôt vexé, et j'explique à un employé qu'il manque 8 700 $ dans mon compte, une somme tout de même rondelette. Je savais ne pas avoir engagé de telles dépenses. L'employé me dit alors que la première étape est de me présenter au détachement local de la GRC ou de la police. Je vous épargne mon expérience de la police locale, mais la GRC s'est révélée très accessible et disponible, et c'est donc là que j'ai signalé la fraude. J'ai rappelé la compagnie émettrice de la carte pour l'aviser que j'avais signalé la fraude, et on m'a heureusement crédité le montant, de sorte que ne n'ai pas eu à assumer la dette. La banque a par la suite trouvé la succursale — située à Edmonton — grâce à un mécanisme de son système et identifié la personne à qui mes fonds ont été transférés.

D'après la greffière du comité, nous inviterons à témoigner les compagnies émettrices de cartes de crédit ainsi que les banques, probablement. Toutefois, les associations avec lesquelles vous faites affaire ont sûrement des codes de pratique à respecter lorsqu'il y a coopération entre les banques et les compagnies émettrices de cartes de crédit, de même qu'à l'égard des services bancaires en ligne. Les mécanismes techniques en place sont-ils efficaces? En existe-t-il de meilleurs?

M. McMahon : Oui, sénateur, les sociétés de télécommunications et les banques travaillent effectivement en étroite collaboration. Elles sont à la fois partenaires et clients. Nous nous occupons souvent de la gestion des réseaux des banques. Nous sommes également victimes de fraudes secteur financier ou ses clients, et ces attaques en ligne sont souvent perpétrées au moyen des infrastructures que nous gérons. C'est donc tout à fait dans notre intérêt commun. Nous nous rencontrons effectivement pour discuter et pour échanger des renseignements, parfois en temps réel.

Il existe deux approches pour traquer les auteurs d'actes tels que la fraude d'identité : suivre l'argent ou suivre les communications. À chaque personne qui fait des opérations en ligne est associée une adresse IP — une adresse de protocole Internet — ou un nom de domaine. Il est possible d'effectuer un suivi financier du parcours des renseignements. Ce ne sont pas nécessairement des systèmes intégrés. L'interface est presque en face à face. Il y aura peut-être un jour un moyen d'établir une corrélation en temps réel pour déterminer où chemine et aboutit l'argent.

Right now, we are doing analysis. Banks do their analysis following fraud and money laundering, and we are doing analysis as to what people are doing bad things on the Internet, where the sources of evil are. The two are being put together at a higher level, an executive summary level, and in some cases, such as in the case of phishing, for instance, we share specific attack factors, such as this attack came from this person or this group.

Senator Dickson: Is there any way this bill could be improved regarding whether or not there is an obligation or an onus on the bank or on Bell Canada to initiative prosecutions, to go to the Mounties and lay a charge?

Mr. McMahon: This is a personal opinion because I am not a legal expert, and I am not speaking for Bell here but mostly for the association.

Nature is sort of taking its course where the critical infrastructures — for instance, communications, telecommunications and finance — recognize that there is a high degree of interdependency and risk associated between the businesses and those two infrastructures. Cooperation is naturally occurring as a result.

The biggest challenges, as I see them, between bringing law enforcement into that is not that we do not talk; we talk every day about the most sensitive issues and on the biggest cases. The challenge is how to get the information in the form it is collected into a form that police forces are accustomed to dealing with in cases. One is looking at bits and bytes travelling across the Internet at huge speeds, and then you are looking at case files. It requires people, processes, technologies and cultural changes to be developed in order to allow that exchange to happen.

Senator Campbell: Is there a concern on your part about obtaining information between peers in a manner that would allow you to take it to court? In other words, you are talking to peers; you are not talking in the context of laying a charge or a criminal offence. You are exchanging information dealing perhaps with crime on the Internet. Is there any concern on your part that that information can then be transferred into the legal system without any difficulties?

Mr. McMahon: The way a telecommunications infrastructure looks at malicious activity is all based upon IP addresses, domain names and technical speak such as that. The actual person at the other end that is perpetrating the crime is not always evident.

Even with respect to the way it is resolved, the help desk will be involved in helping resolve incidents of a malicious nature, and it tends to be based upon IP addresses and user accounts, things like that. It is not necessarily in a format that lends itself to easy prosecution or the way the RCMP would look at something, such as a crime took place and this is how we want to go about prosecuting. In many cases, it is easier to stop the attack than to

Des analyses sont en cours. Les banques analysent la fraude et le blanchiment d'argent, et nous nous intéressons aux actes malveillants commis sur Internet pour déterminer d'où provient le mal. Les deux analyses sont mises en commun à un niveau supérieur, dans un résumé. Dans certains cas, notamment lorsqu'il est question d'hameçonnage, nous communiquons des données spécifiques, telles que la personne ou le groupe à l'origine de l'attaque.

Le sénateur Dickson : Y a-t-il moyen d'améliorer le projet de loi pour mieux préciser si une banque ou Bell Canada a l'obligation ou la responsabilité d'intenter une poursuite judiciaire, de faire appel à la GRC et de porter une accusation?

M. McMahon : Ce que je m'apprête à dire n'est que mon opinion personnelle parce que je ne suis pas un juriste, et je ne parle pas au nom de Bell, mais principalement comme porte-parole de l'association.

La nature semble suivre son cours. Les principaux secteurs à risque — par exemple, les communications, les télécommunications et la finance — reconnaissent la forte interdépendance et le risque élevé qui découlent des liens entre les entreprises et ces deux infrastructures. En conséquence, la coopération se fait naturellement.

D'après moi, le plus grand obstacle à l'inclusion des organismes d'application de la loi n'est pas l'absence de dialogue; nous avons des échanges quotidiens au sujet des problèmes les plus graves et des plus grands dossiers. Le défi consiste à trouver un moyen de présenter les données recueillies sous une forme utile aux services de police, dans le cadre de leurs enquêtes. Il faut adapter les renseignements concernant les bits et les octets qui parcourent le cyberespace à une vitesse fulgurante pour qu'ils ressemblent à ceux que l'on retrouve habituellement dans le dossier d'une affaire, ce qui requiert de la main-d'œuvre, des processus et des technologies. Il faut également changer les façons de penser.

Le sénateur Campbell : La possibilité de présenter comme preuve devant un tribunal des renseignements échangés entre pairs vous préoccupe-t-elle? En d'autres mots, vous discutez simplement avec vos collègues, sans qu'il soit question de porter des accusations, au criminel ou non. Il est possible que vous échangiez des renseignements potentiellement liés à une cyberfraude. Vous inquiétez-vous du fait que ces renseignements peuvent facilement servir de preuve devant les tribunaux?

M. McMahon : Lorsque les sociétés de télécommunications traitent d'actes malveillants, elles utilisent du jargon informatique et parlent d'adresses IP, de noms de domaine, et ainsi de suite. Il n'est pas toujours évident d'identifier l'auteur du crime.

Même dans sa façon de régler les problèmes, le service de dépannage aide à résoudre des incidents de nature malveillante souvent en fonction des adresses IP et des comptes utilisateur, par exemple. L'information n'est pas nécessairement dans un format qui se prête à une accusation facile ou que la GRC peut examiner facilement pour déterminer s'il y a eu crime et comment procéder à la mise en accusation de son auteur. Il est souvent plus facile de

figure out who is causing it. In many cases, if there is a massive attack coming from another country, you would block that attack rather than try to investigate who is behind it and why.

Senator Campbell: The only question I have is regarding going forward to try to stop these attacks. There was a phrase used in legal investigative circles many years ago, "I will show you mine and you show me yours," and it was not from a point of view of laying a charge so much as it was sharing information in order to continue on the investigation, and that information in fact would never form part of your charge. Is that the kind of situation you find yourself in?

I get the sense you are at a much higher level with just the IP addresses and domains, and your concern is more about stopping an attack coming through your network than it is about actual criminal charges or catching someone; your concern is more based on business.

Mr. McMahon: I think that is correct. If one of our subscribers or clients is behaving poorly, then there is a fairly easy way of dealing with it because we know who it is and we will be able to take that to the authorities, if not deal with it directly with the client.

The other issue refers to criminal intelligence, whether that is environmental scanning in developing a situation. A typical example would be a police force asking about what is happening in the criminal intelligence world with regards to cyber crime. Who are the bad guys? We need enough information so we can start an investigation because we do not know who to look for.

That is a great deal of discussion, as it would start, let us say, with publishing a white paper or publishing threat reports on a macro-scale, eventually getting down to the point where there is enough information that the RCMP can use it within an investigation, at which point there will be a cut-off. When you start asking for specific people's names and Canadians are involved, a warrant is sought and it enters into an investigative stage.

The first page of that stage would not be dealing with private information, but more dealing with means, motives, methods and perhaps identifying threat groups, locations and things like that.

The stuff in the middle is always a matter of discussion because that is where one must tread carefully in terms of satisfying the needs of law enforcement with developing a background for an investigation, the privacy needs of citizens and the neutrality in the middle. That is where a lot of the discussion happens between legal groups and operational groups.

Senator Bryden: I would like to follow up and ask one question. High-speed Internet connection can be accessed by land line, but it can also be accessed by satellite. Is one of those two

stopper l'attaque que d'en déterminer la source. En effet, il est plus facile de contrer une attaque massive venue de l'étranger que d'enquêter sur son origine ou le motif.

Le sénateur Campbell : Ma dernière question concerne ce que nous pouvons faire à l'avenir pour arrêter les attaques. Il y a longtemps, dans les cercles d'enquête judiciaire, on utilisait une expression du genre « Je vais vous dévoiler mes renseignements si vous me rendez la pareille. » Un pareil échange d'information avait pour but principal le partage de renseignements afin de poursuivre l'enquête. Ils n'étaient pas particulièrement destinés à servir de preuve dans un procès. Vous trouvez-vous dans une situation semblable?

J'ai l'impression que vous évoluez dans une plus haute sphère, dans un monde plus virtuel de simples adresses IP et noms de domaines. Vous semblez plus intéressé à stopper une attaque contre votre réseau qu'à porter une accusation criminelle ou arrêter quelqu'un; vous êtes davantage préoccupé par la protection d'intérêts commerciaux.

M. McMahon : Je crois que vous misez juste. Si l'un de nos abonnés ou clients se conduit mal, il est plutôt facile de régler le problème parce que nous savons exactement de qui il s'agit et que nous pouvons fournir son identité aux autorités ou même nous en occuper directement avec le client.

L'autre question porte sur les renseignements criminels, à savoir la recherche de données sur l'évolution d'une situation. Prenons l'exemple d'un service de police qui demande à avoir des renseignements criminels reliés aux crimes cybernétiques. Qui sont les criminels? Nous avons besoin d'information avant de pouvoir lancer une recherche parce que nous ignorons où la commencer.

Beaucoup de discussions précèdent, par exemple, la publication d'un livre blanc ou de rapports sur la menace à grande échelle, jusqu'à ce que la GRC ait suffisamment de renseignements qu'elle peut utiliser dans le cadre d'une enquête. C'est à ce stade que notre recherche prend fin. De fait, lorsque l'on commence à demander les noms de personnes spécifiques ou de Canadiens impliqués, la GRC demande un mandat et entame son enquête.

Donc, la première partie de la recherche ne porte pas sur des renseignements privés; il est plutôt question d'identifier les moyens, les motifs et les méthodes ainsi que de cibler les groupes constituant une menace, l'endroit où ils se trouvent, et ainsi de suite.

Ce qui se passe dans l'intervalle reste matière à discussion parce que c'est là où il faut avancer avec précaution, car il faut satisfaire aux besoins de l'application de la loi tout en développant un contexte pour une enquête, en respectant les exigences en matière de vie privée des citoyens et en restant neutre. C'est autour de cette question que tournent beaucoup de discussions entre les groupes juridiques et opérationnels.

Le sénateur Bryden : J'aimerais enchainer en vous posant une question. On peut avoir accès à Internet haute vitesse par ligne terrestre, mais aussi par satellite. L'un des deux modes de

modes more prone to attack? Is it easier to attack satellite mode than land line mode or vice versa?

Mr. McMahon: That is an excellent question. If you are trying to take over a computer, you want a computer that is nice and fast. You do not want to necessarily steal the identity, but you want to use it as a launching point for things like quick fraud, spam runs and things like that. If you get the person's identity in the meantime, that is a bonus, but you are looking at using the computer as a launching platform. You would therefore want bandwidth.

On the other hand, you have to be able to take over the machine. Some of the most un-patched machines are actually dial-up because it takes such a long time to download all the latest patches; they therefore tend to be un-patched machines.

On the one hand, we see a lot of dial-up connections that are infected, and that is balanced with high bandwidth connections and powerful machines that are infected but for two completely different reasons. As dial-up becomes less obvious, we will see a bump in high bandwidth solutions providing the biggest threat, with the most malicious traffic. The next bump will be the introduction of broadband, high-speed, 4G systems which appear on hand-held devices in order to operate at fast speeds. We suspect that will also add to some of the noise.

Senator Bryden: Could I get an answer to my question? Is it more risky for me to have a dial-up, which is what I have now because that is all I can get, than satellite feed into my house? Do you know?

Mr. McMahon: I do not know precisely. I would suggest that it probably would be very similar. We have only noticed the other observation about dial-up versus broadband connections. I have not made the assessment between satellite and DSL connections.

The Chair: I will ask senators and Mr. McMahon to be as concise as we can because we have more witnesses to hear from this interesting morning and we will soon bump up against a Senate sitting, at which point we must adjourn this meeting.

Senator Baker: Since we are on television and we have the author with us, I wanted to say that I think the book is called *Cyber Crime*. Is that the name of your book?

Mr. McMahon: *Cyber Threat*.

Senator Baker: It is an excellent book, written in layman's language. Everyone can understand it. It would make a great Christmas present for someone.

My question to you is this: You referenced in each question put to you by the senators the effect of the bill. Yes, in one case you said that it certainly will not do any harm, and so on. Of course, your point is well-taken that much of the crime occurs outside the borders of Canada. Have you given any thought or what would you say to the committee as far as there being a provision in this bill applying to prosecutions outside of the country that use

connexion est-il plus vulnérable aux attaques? Est-il plus facile d'attaquer une connexion par satellite qu'une connexion par ligne terrestre ou l'inverse?

M. McMahon : C'est une excellente question. Un pirate informatique qui tente de prendre le contrôle d'un ordinateur veut avoir accès à un bon ordinateur qui est rapide. Il ne cherche pas spécialement à voler l'identité de l'usager; il utilise plutôt l'appareil comme point de lancement pour commettre une fraude rapide et envoyer des pourriels, par exemple. S'il réussit à voler l'identité de l'usager par la même occasion, c'est une prime, mais son but premier est d'utiliser l'ordinateur comme plateforme de lancement. Ainsi, il cherchera à avoir une bonne bande passante.

Cependant, il lui faut également être en mesure de prendre le contrôle de l'ordinateur. Les ordinateurs qui ont un accès Internet par réseau commuté sont souvent les moins à jour parce que le téléchargement des rustines récentes prend une éternité.

On remarque donc que beaucoup d'ordinateurs à accès commuté sont infectés, mais il semble que les connexions à large bande passante et les ordinateurs puissants sont également infectés pour deux raisons tout à fait différentes. Comme l'accès commuté tend à disparaître, les solutions à large bande passante — qui constituent la plus grande menace — augmenteront en nombre et, de ce fait, le trafic le plus malveillant. L'autre choc surviendra à l'entrée sur les marchés des systèmes 4G — offrant Internet haute vitesse à large bande — qui sont intégrés dans les appareils portatifs pour accélérer leur vitesse. Nous estimons que ces deux éléments aggraveront le phénomène actuel.

Le sénateur Bryden : Je ne crois pas que vous ayez répondu à ma question. Est-ce plus risqué d'avoir un accès commuté à la maison — ce que j'ai actuellement parce que c'est le seul service disponible chez moi — qu'un accès satellite? Le savez-vous?

M. McMahon : Je n'en suis pas certain. À mon avis, c'est probablement très semblable. Nous avons fait la comparaison entre un accès commuté et un accès à large bande passante, mais pas entre une connexion satellite et une connexion DSL.

La présidente : Je demanderais aux sénateurs et à M. McMahon d'être le plus concis possible parce que nous avons d'autres témoins à entendre ce matin et qu'il nous faudra bientôt lever la séance pour nous rendre à la Chambre du Sénat.

Le sénateur Baker : Comme notre séance est télédiffusée et que nous avons l'auteur avec nous, je voudrais rappeler que le livre s'intitule *Cyber Crime*. Est-ce bien le titre de votre livre?

M. McMahon : Il s'intitule *Cyber Threat*.

Le sénateur Baker : C'est un excellent livre, bien vulgarisé et à la portée de tous. C'est une très bonne suggestion cadeau pour Noël.

J'aimerais vous demander ceci : À chaque fois que vous avez répondu aux questions des sénateurs, vous avez parlé des répercussions du projet de loi. Dans un cas, vous avez effectivement affirmé qu'il n'y aurait pas de retombées négatives. Vous avez bien sûr fait valoir que la majorité des crimes sont perpétrés à l'extérieur des frontières du Canada, et nous le comprenons bien. Pouvez-vous proposer au comité une

identities that are obtained within the country? According to you, that involves the majority of identity theft with which we are dealing.

Mr. McMahon: That is an interesting question, senator. I have given a lot of thought to how to tackle the problem. I have not considered legislative instruments and legal instruments as being a huge part of that, mostly because my sphere of control and influence is mostly on the technological side as opposed to the legal side.

I can say only that I have been involved in conversations where my legal colleagues have been perplexed or upset about the lack of power they have to prosecute or even investigate cases abroad. In some cases, the solution has been that it is more pragmatic to stop the attacks and identify the attacks rather than to try to go after them after the fact. There are also many discussions about how one might go about carrying on those cases abroad.

Senator Wallace: I would like to come back to a point that Senator Joyal made earlier. It was a good point. With your technological background, I am sure it is one that would mean a lot to you. As we move forward to deal with this issue of identity theft, we should not limit ourselves to the technologies that we know today; we should leave it more open than that. That makes sense.

In my reading of Bill S-4 and, in particular, the definition of ''identity information'' and how that relates to identity theft, I do not believe that it is limited to any medium in which that information is stored or to any particular technology. I thought from your comment earlier that you would agree with that, but I wanted to confirm that. Is there anything in the bill that you feel limits the scope of technology in defining what would constitute identity information?

Mr. McMahon: I personally do not think so. My experience over the last couple of decades dealing with the legal community is that some lawyers would be very creative and find a way to prosecute within the bounds of the written law; others would interpret it differently and in a very risk-averse manner.

Senator Wallace: We will follow your opinion, I think.

Senator Milne: You have described to us that crime is really moving from identity theft and credit card or debit card threat increasingly to methods over the Internet of stealing $1 from one million accounts instead of large amounts from a few accounts. I simply cannot see how either the police or you will ever be able to track this kind of crime. The people or the companies who have the money stolen from their accounts will not even realize. A $10 amount here or there happens; people can forget how much they have.

disposition à inclure au projet de loi qui s'appliquerait aux poursuites à l'étranger pour l'utilisation d'identités volées au Canada? Selon vous, la majeure partie des vols d'identités auxquels nous avons affaire sont commis à l'extérieur du pays?

M. McMahon : C'est une question intéressante, monsieur le sénateur. J'ai beaucoup réfléchi pour trouver un moyen de régler le problème. Je n'ai pas envisagé de mesures législatives comme principale solution, surtout parce que mon champ de compétence et d'influence se limite plutôt au domaine technologique, et non pas au domaine juridique.

Je peux cependant vous affirmer que des collègues avocats m'ont dit être dépassés ou frustrés par le peu de pouvoirs qu'ils ont de porter des accusations ou même de faire enquête à l'étranger. Il s'avère parfois plus pragmatique de tenter de stopper et de cerner la provenance des attaques au lieu de s'en prendre aux responsables après-coup. Il est par ailleurs souvent question de la façon dont on pourrait poursuivre ces dossiers à l'étranger.

Le sénateur Wallace : J'aimerais revenir à un point qu'a soulevé le sénateur Joyal un peu plus tôt. C'était une question très pertinente. Vu l'étendue de vos connaissances technologiques, je suis persuadé que vous comprendrez parfaitement de quoi il en retourne. Si nous voulons régler ce problème de vol d'identité, nous ne pouvons pas nous limiter aux technologies que nous connaissons aujourd'hui; il faut prévoir une certaine marge de manœuvre. Cela me paraît logique.

Quand je lis le projet de loi S-4, et particulièrement la définition de « renseignements identificateurs » et le rapport établi avec le vol d'identité, je n'ai pas l'impression qu'on se limite à un quelconque support de stockage des données ni à une technologie particulière. J'ai cru comprendre, d'après les propos que vous avez tenus, que vous abondiez aussi dans ce sens, mais je voulais seulement le confirmer. À votre avis, est-ce que quelque chose dans le projet de loi restreint la portée de la définition de « renseignements identificateurs »?

M. McMahon : Je ne crois pas personnellement que ce soit le cas. Je vous dirais cependant, si je me fie à mes 20 années d'expérience avec le milieu juridique, que certains avocats sauraient user d'imagination pour porter des accusations dans les limites du texte législatif; d'autres l'interpréteraient différemment et très prudemment.

Le sénateur Wallace : Je crois que nous allons suivre votre opinion.

Le sénateur Milne : Vous nous avez expliqué que le vol d'identité et la fraude par carte de crédit ou de débit laissent de plus en plus la place à des méthodes visant à voler 1 $ dans un million de comptes bancaires sur Internet, plutôt que de voler de gros montants dans quelques comptes. Je ne vois pas comment la police ou vous-même allez pouvoir détecter ce genre de crime. Les gens ou les compagnies qui auront été la cible de ces fraudes ne s'en rendront même pas compte. Un écart de plus ou moins 10 $ ne se remarque pas nécessairement; les gens peuvent oublier le montant exact qui se trouve dans leur compte.

The bill addresses a type of crime that will be decreasing rather than increasing. I cannot see that those million people who have had $10 stolen from them will ever complain or even realize it. I am beginning to realize what will be the effect of this bill.

Mr. McMahon: That is a very insightful observation. I think that what it does tell is that the traditional way of finding one victim — that is, someone sitting at home that has their bank account raided — will shift towards, in a typical case, going after and identifying an organization within Canada. For example, there is a celebrated case in Montreal where none of the victims were aware that they were victims, but, through other investigative means, the police were able to identify that a group had stolen tens of thousands and millions of credit card information and were using it.

This bill would allow them to prosecute that case. The challenge, from what I have heard articulated to me, is that the police have difficulty informing all those victims and then bringing them all to court to testify. It would be much easier if they could bring the people they are intending to prosecute to court and ask them to explain why they had a million credit card numbers sitting on their computer.

The target of the crime will not be based on a victim complaining but, rather, on some very active, pro-active policing, I think.

Senator Milne: A previous incarnation of this committee heard from the online gambling people that IP providers, service providers and telephone companies were really just facilitators. They were not talking to the police. However, we are now hearing from you that you are talking to the police all the time. I am beginning to wonder exactly what the situation is.

Mr. McMahon: It varies between police forces and between various telecommunications companies. When you are looking at tier one carriers and main national police forces, there is good cooperation. If you are looking at a tier three provider and a local police force, I cannot speak to how good their relations are.

The Chair: It gets more and more interesting, but our time has run out, Mr. McMahon. We thank you very much. This has been extremely useful, as Senator Baker observed, all in language that we could understand, which is very helpful.

We are now pleased to welcome, from the Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic, Mr. David Fewer, Acting Director; and Mr. Tamir Israel, articling student.

I believe you know how we operate. We ask you to make an opening statement and then we will go to questions.

Le projet de loi vise un genre de crime qui a tendance à diminuer plutôt qu'à augmenter. Je ne crois pas que ce million de personnes à qui on a volé 10 $ ne vont jamais se plaindre ou même réaliser ce qui s'est passé. Je commence à comprendre quel sera l'impact de ce projet de loi.

M. McMahon : C'est une observation très perspicace. Cela nous révèle en fait que la façon traditionnelle de trouver une victime — c'est-à-dire un consommateur qui se fait attaquer son compte en banque tandis qu'il est à la maison — ne sera plus la même; on préférera plutôt cibler une organisation précise au Canada. Dans une affaire désormais célèbre à Montréal, aucune des victimes ne savaient qu'elles avaient été ciblées, mais, grâce à d'autres méthodes d'enquête, la police a découvert qu'un groupe avait volé et utilisait des dizaines de milliers, voire des millions, de n^{o}s de carte de crédit.

Ce projet de loi permettrait à la police de porter des accusations dans ce dossier. Ce qui pose problème, d'après ce qu'on m'a dit, c'est que la police a de la difficulté à informer toutes les victimes et à les amener à témoigner en cour. Il serait beaucoup plus facile si elle pouvait traîner devant les tribunaux les personnes qu'elle veut poursuivre pour leur demander d'expliquer pourquoi des millions de n^{o}s de carte de crédit se trouvaient dans leur ordinateur.

J'ai l'impression que les criminels ne seront pas retracés grâce à des plaintes formulées par les victimes, mais grâce à des techniques très proactives de maintien de l'ordre.

Le sénateur Milne : Dans une législature précédente, des témoins du secteur du jeu en ligne ont dit à ce comité que les fournisseurs d'adresses IP, les fournisseurs de services et les compagnies téléphoniques étaient ni plus ni moins des facilitateurs. On soutenait que ces derniers ne parlaient pas à la police. Vous nous apprenez toutefois aujourd'hui que vous êtes continuellement en communication avec la police. Je commence à me demander ce qu'est la situation exactement.

M. McMahon : Cela varie d'une entreprise de télécommunications à l'autre, et d'un service de police à l'autre. On peut dire qu'il y a une bonne coopération entre les fournisseurs de premier niveau et les principaux corps policiers. Je ne sais cependant pas quelles sont les relations entre les fournisseurs de troisième palier et les corps policiers locaux.

La présidente : Cela devient de plus en plus intéressant, monsieur McMahon, mais notre temps est écoulé. Merci beaucoup. Votre témoignage nous sera très utile et, comme l'a fait remarquer le sénateur Baker, vous avez su vulgariser vos propos, ce qui nous aide aussi beaucoup.

C'est avec plaisir que nous accueillons maintenant, de la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko, M. David Fewer, directeur intérimaire, et M. Tamir Israel, stagiaire en droit.

Je crois que vous savez comment les choses se déroulent. Nous vous demandons de faire une déclaration préliminaire avant de répondre à nos questions.

David Fewer, Acting Director, Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic: Thank you for the opportunity to bring us here to speak about a serious problem that is directly affecting an increasing number of Canadians. It is indirectly affecting us all through the costs that are passed on to consumers and through the preventative measures that we all now must take.

Our clinic is a technology clinic at the law faculty at the University of Ottawa. Our mandate is to speak on behalf of the public interest at the intersection of law and technology. You can understand why we are here today.

We have done a great deal of work in this area in the past. We have been part of a multi-institution research project on identity theft that is now completed but was funded by the Ontario Research Network for Electronic Commerce, which is a private-public partnership that includes four major Canadian banks. Over the course of the last four years, we have been researching legal and policy initiatives in this area. Colleagues at four other Ontario universities have also been examining issues involved in the definition and measurement of identity theft, as well as approaches to technological solutions to ID theft.

On our website, at cippic.ca, we have published a series of working papers on various aspects of ID theft. These include an introduction and backgrounder, a working paper on techniques, a working paper on legislative approaches to identity theft, an overview of case law on identity theft, policy approaches to identity theft and enforcement of identity theft laws.

We have also published a white paper on security breach notifications, which we would say is one measure that the Canadian government could be taking steps on that would help address identity theft issues quite apart from what we are here today to speak about.

We have also posted a web page on identity theft that includes all these documents and more, in addition to frequently asked questions and resources for the public. Later this year, we will issue a final white paper that tries to pull together all of this work with specific recommendations for law reform and for policy reform.

We are pleased to address you today on the topic of Bill S-4. Our comments will touch on three topics: first, Bill S-4's proposed changes to the Criminal Code; second, some proposed changes to the Criminal Code that are not in Bill S-4 but would go a long way, we think, towards helping to address identity theft issues; and, finally, wider proposals to address identity theft.

I saw from the grilling that you gave my friend Mr. McMahon this morning that you have a lot of questions on this topic. I propose that I will abbreviate the comments that I was going to give and get right to it.

David Fewer, directeur intérimaire, Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko : Merci de nous avoir invités pour vous parler d'un grave problème qui touche directement de plus en plus de Canadiens. C'est un problème qui nous touche tous indirectement compte tenu des coûts qui se répercutent sur les consommateurs et des mesures préventives que nous devons maintenant prendre.

Nous dirigeons une clinique technologique établie à la Faculté de droit de l'Université d'Ottawa. Notre mandat est de défendre l'intérêt public, à la croisée du droit et de la technologie. Vous comprenez maintenant pourquoi nous sommes ici.

Nous avons beaucoup travaillé dans ce domaine dans le passé. Nous avons pris part à un projet de recherche multipartite sur le vol d'identité, qui est maintenant terminé et qui avait été financé par l'Ontario Research Network for Electronic Commerce, un partenariat public-privé auquel quatre grandes banques canadiennes se sont associées. Depuis quatre ans, nous examinons des initiatives juridiques et politiques dans ce domaine. Des collègues de quatre autres universités ontariennes se sont aussi penchés sur des questions touchant à la définition et à la mesure du vol d'identité, de même que sur des solutions technologiques pour contrer ce genre de vol.

Sur notre site web, au cippic.ca, nous avons publié une série de documents de travail sur différents aspects du vol d'identité. Vous y trouverez notamment une introduction et une fiche documentaire, ainsi qu'un document de travail sur les différentes techniques, un document de travail sur les approches législatives visant à cerner ce genre de vol, de même qu'un aperçu de la jurisprudence sur le vol d'identité, des approches politiques pour détecter le vol et de l'application des lois portant sur le vol d'identité.

Nous avons aussi publié un livre blanc préconisant la notification des atteintes à la sécurité, une mesure que le gouvernement canadien pourrait prendre en vue de remédier au problème du vol d'identité, en plus des moyens dont nous voulons vous parler aujourd'hui.

Nous avons par ailleurs publié une page web sur le vol d'identité qui comprend tous ces documents et bien d'autres, en plus d'une foire aux questions et des ressources à l'intention du public. Plus tard cette année, nous allons publier la version finale de notre livre blanc, qui fait la synthèse de l'ensemble de notre travail et qui formule des recommandations précises au sujet de réformes législatives et politiques.

Nous sommes heureux de venir vous parler du projet de loi S-4 aujourd'hui. Nous aborderons trois sujets : les changements que propose le projet de loi S-4 au Code criminel; des changements au Code criminel que ne prévoit pas le projet de loi S-4, mais qui contribueraient grandement, à notre avis, à remédier au problème du vol d'identité; ainsi que des propositions d'ordre général pour contrer le vol d'identité.

À la façon dont vous avez interrogé mon ami, M. McMahon, ce matin, j'en déduis que vous avez beaucoup de questions à poser sur le sujet. Je propose d'abréger mes remarques préliminaires pour que nous puissions passer plus rapidement à la ronde de questions.

Our position on Bill S-4 is that we like it. This is good. Bill S-4 addresses wrongful activities and fills gaps in the current law with respect to preparatory acts involved in identity theft — thumbs up. It will also provide law enforcement authorities with much better legislative tools with which to catch and convict identity thieves. Again, thumbs up. We are particularly pleased with the amendment providing for victim restitution.

What is not in the bill? I do not want the Canadian government to pass this bill, this law, and think, "Okay. We are done with identity theft. We have done what we can do." This is just the beginning. This bill goes a long way in saying that these acts are wrongful. They are contrary to the Criminal Code and we have measures in place for law enforcement to address them, but much more could be done, even within the Criminal Code.

We would like to see amendments to the Criminal Code to provide for victims to have the right to obtain a police report. This will go a long way towards helping victims follow up with law enforcement agencies and do away with an impediment to the fast action that is required for victims to repair damage and prevent further damage. That is one of the interesting things about identity theft. It is the crime that keeps giving or taking, again and again.

Second, we would like to see the Criminal Code amended to provide for the right of a victim to obtain a court order indicating factual innocence. Again, this goes to the point that victims of identity crime have to go back again and again to creditors, to banks, and to other institutions that they are dealing with saying, ''No, that was not me. I am a victim of this crime the same way that you are.'' A court order declaring innocence would go a long way towards helping victims address those issues.

Finally, we would like to see stronger sentencing guidelines developed for offences involving identity fraud. Our observation has been, particularly earlier in the evolution of this crime, that penalties were relatively low. The attraction for organized crime in particular to regard these sorts of penalties as the cost of doing business is just unacceptable. We would like to see guidelines on sentencing that show that this is in fact a harmful crime and that those convicted should be sentenced to significant penalties.

Finally, with respect to extra criminal measures, we really want to emphasize that the Criminal Code is capable of addressing only a small part of the identity theft problem. If we are to attack the problem of identity theft effectively, we need to do much more than just establish crimes for which police can charge offenders. First and foremost, we think there is a need for better data. We have a difficult time in Canada getting an understanding of the scope of the problem, the quantum of harm, and the length of

Nous appuyons le projet de loi S-4. C'est très bien. Le projet de loi S-4 vise des activités frauduleuses et comble des lacunes dans la législation actuelle en ce qui a trait aux actes qui constituent la première étape du vol d'identité. Bravo. Il fournit également aux autorités responsables de l'application de la loi de biens meilleurs outils législatifs pour arrêter les voleurs d'identité et les faire déclarer coupables. Encore une fois, bravo. Nous sommes particulièrement satisfaits de l'amendement prévoyant un dédommagement des victimes.

Qu'est-ce qui fait défaut au projet de loi? Je ne voudrais pas que le gouvernement du Canada adopte ce projet de loi en se disant que cela réglera le problème du vol d'identité et qu'il a fait ce qu'il avait à faire. Ce n'est que le commencement. Ce projet de loi permettra d'accomplir beaucoup en reconnaissant qu'il s'agit d'actes frauduleux. Nous reconnaissons qu'ils sont contraires au Code criminel et nous avons des mesures en place pour faire appliquer la loi, mais nous pouvons en faire encore plus, même dans les limites du Code criminel.

Nous aimerions que des modifications soient apportées au Code criminel afin que les victimes aient le droit d'obtenir un rapport de police. C'est une mesure qui aiderait énormément les victimes à assurer un suivi auprès des organismes d'application de la loi, et qui leur permettraient de réagir plus rapidement afin de réparer les dégâts et de prévenir une nouvelle attaque. C'est une des choses intéressantes à propos du vol d'identité. C'est un crime qui n'arrête jamais de frapper.

Nous aimerions aussi que le Code criminel soit modifié pour accorder aux victimes le droit d'obtenir une ordonnance de la cour déclarant leur innocence réelle. C'est encore là pour aider les victimes à faire valoir aux créditeurs, aux banques et aux établissements avec lesquels elles font affaire qu'elles n'ont rien à voir avec les fraudes commises. Une ordonnance de la cour les aiderait grandement dans leurs démarches.

Finalement, nous aimerions que soient établies des lignes directrices régissant l'imposition de peines plus sévères dans les cas de fraudes d'identité. Nous avons remarqué, particulièrement à l'époque où l'on commençait à voir de plus en plus ce genre de crimes, que les juges imposent des peines relativement légères. Le crime organisé pourrait traiter une telle peine simplement comme un coût lié à la « conduite des affaires », ce qui est carrément inacceptable. Nous voulons que des lignes directrices soient établies pour montrer qu'il s'agit d'un crime grave et que les personnes déclarées coupables se voient imposer des peines dissuasives.

Enfin, pour ce qui ce qui est des mesures extra criminelles, nous tenons à souligner que le Code criminel ne peut régler qu'une toute petite partie du problème. Si nous voulons le combattre de façon efficace, nous devons faire beaucoup plus qu'établir des crimes pour lesquels la police peut donner des accusations contre les contrevenants. Nous croyons qu'il faut d'abord et avant tout disposer de meilleures données. Il est difficile au Canada de bien comprendre toute l'ampleur du problème, le quantum des

harm associated with identity theft. We think we can do much more in gathering that data.

The primary means to do so, in my view, would be the establishment of a federal-provincial-territorial task force on addressing identity crime issues. This approach was adopted in other jurisdictions and has resulted, in my view, in a much more comprehensive and coherent policy approach to dealing with identity theft. Canada should follow those approaches. We have done so before in other contexts, particularly with respect to the anti-spam task force a few years ago that has now resulted in Bill C-27 before the House of Commons, which addresses not only spam but also other privacy-related online threats, such as spyware.

Second is resources. My guess is that this committee has heard or will be hearing from law enforcement who will tell you that having the resources, both the technological expertise and the financial resources, to address identity theft issues is an impediment to the resolution.

Third is addressing sources. This is a huge issue. If it were not so easy to get consumer information to commit identity theft, it would not be such a problem for consumers. This means, to a certain extent, that consumers must be more aware of what they can do to limit identity theft, but it also means addressing the institutions and organizations that hold consumer data. We could do a lot more in the area of security breach. What kind of obligations are on institutions to safeguard all of our personal data? What kind of obligations do they have to disclose to consumers when a breach occurs? To whom should that disclosure occur? We can do a great deal in this area.

Fourth is mitigation. I have touched upon this a bit with respect to the scope for mitigation provisions within the Criminal Code, but I think we can do more as well. Consumers should be given rights empowering them to mitigate damages when they find themselves victimized or at risk of being victimized. For example, we should have the right to be informed of a security breach issue. Right now, we are not.

I was interviewed by the CBC just a few days ago and found out that credit card companies do not tell consumers where the source of a breach has occurred, if there has been a breach at a business they deal with, and this is because credit card companies are in an inherent conflict of interest. They have a double-sided business. Consumers are the customers, but the businesses consumers deal with are also their customers, and the credit

dommages causés, et la durée sur laquelle s'étend les dommages associés au vol d'identité. Nous pensons que nous pouvons en faire beaucoup plus en ce qui a trait à la collecte de données.

La meilleure façon pour y arriver, selon moi, est d'établir un groupe spécial fédéral-provincial-territorial chargé d'étudier les questions liées au vol d'identité. Cette façon de faire a été adoptée ailleurs dans le monde et a permis d'arriver à une approche politique plus complète et cohérente pour s'attaquer au problème. Le Canada devrait suivre la même démarche. Nous l'avons fait auparavant dans d'autres contextes, notamment avec le groupe de travail anti-pourriel il y a quelques années, qui a mené au dépôt du projet de loi C-27 devant la Chambre des communes; il s'agit d'un projet de loi qui vise non seulement les pourriels, mais aussi les autres menaces liées à la confidentialité, comme les logiciels espions.

Il faut ensuite prévoir des ressources. Je présume que le comité a déjà entendu des témoins représentant des organismes d'application de la loi, ou il le fera sous peu. Ces derniers vous diront qu'ils n'ont tout simplement pas les ressources nécessaires, tant au plan de l'expertise technologique que des ressources financières, pour être en mesure de remédier à la situation et de contrer le vol d'identité.

Il ne faut pas non plus oublier de s'attaquer aux sources d'information, ce qui constitue une difficulté énorme. S'il n'était pas aussi facile d'obtenir les renseignements des consommateurs pour commettre des vols d'identité, le problème n'aurait certainement pas la même ampleur. Cela signifie, dans une certaine mesure, que les consommateurs doivent être mieux informés des mesures qu'ils peuvent prendre pour prévenir le vol d'identité. Mais il faut également regarder du côté des établissements et des organisations qui détiennent des données sur les consommateurs. Nous pourrions en faire beaucoup plus pour déjouer les atteintes à la sécurité. Les établissements ont-ils l'obligation de protéger nos renseignements personnels? Ont-ils l'obligation d'aviser les consommateurs en cas de violation de la sécurité des ordinateurs? À qui cet avis devrait-il être émis? Nous avons encore du chemin à faire dans ce domaine.

Nous devons en outre penser à l'atténuation des dommages. J'ai abordé brièvement le sujet en parlant des dispositions en ce sens à inclure au Code criminel, mais je continue de croire que ce n'est pas suffisant. Les consommateurs devraient avoir des droits les aidant à atténuer les effets du crime dont ils ont été victimes et à réduire les risques de se faire prendre. Par exemple, nous devrions avoir le droit d'être informés de toute brèche de sécurité. C'est un droit que nous n'avons pas à l'heure actuelle.

J'ai donné une entrevue à la CBC il y a quelques jours, et j'ai découvert que les compagnies émettrices de cartes de crédit ne le disent pas aux consommateurs si une brèche de sécurité s'est produite dans un commerce avec lequel elles font affaire. Les compagnies agissent ainsi parce qu'elles se retrouvent en situation de conflit d'intérêts inhérent. Elles ont une entreprise à double face. Les consommateurs sont leurs clients, mais les entreprises

card industry does not have an interest in disclosing which of its customers has a compromised security breach area. We can do more.

The finally point is an identity theft victim assistance bureau. If you have ever met or spoken to someone who has been a victim of identity theft, you know it is a very difficult process to remediate. We could do an awful lot to help victims in this area, and I do not think we are doing anywhere near enough.

Those are my initial comments. I would welcome questions on any of those things, and, obviously, of course, on Bill S-4 as well.

The Chair: Thank you very much indeed.

Senator Wallace: I compliment you on the detailed work that you have done, the comprehensive review that you have given this topic and the studies that are online. Certainly we will be looking at those.

I was interested to hear you say that the work that you have done has involved the banks. Of course, the banks are greatly concerned and are really at the front line of identity theft. As Senator Dickson pointed out earlier, being a victim of credit card fraud puts you in direct contact with your banks. They hear the complaints and deal with the financial reality of it. I am curious about the response that you have heard directly from the banks in regards to Bill S-4. I have had discussions with them, and I wonder how you find their reaction to this bill and the level of support they have for this bill.

Mr. Fewer: I have not heard any opposition to the bill from the banks, not directly, though I do have to confess that I personally have not discussed this issue with the banks, this legislation or Bill C-27 before it, or even Bill C-299, the impersonation bill that preceded this one as well.

Tamir Israel, Articling student, Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic: I do not think we consulted with the banks on this.

Mr. Fewer: I do not have a great answer for you on that.

I should introduce Tamir Israel, SCIPPIC staff. He has done a great deal of work in the area of confidential information and personal information and has an interest in identity theft.

Senator Wallace: Thank you. With many of the recommendations that you have made and included in your presentation and the analysis you have done, have you had a detailed analysis of other jurisdictions? Have you looked at how they have dealt with the issue, and does that form part of the basis of the opinion you shared with us this morning?

avec lesquelles traitent les consommateurs sont aussi leurs clientes. L'industrie des cartes de crédit n'a donc pas intérêt à divulguer lequel de ses clients a été la cible d'une telle violation. Il faut prendre des mesures à cet égard.

Finalement, nous recommandons d'établir un bureau d'aide aux victimes. Si vous en avez déjà discuté avec moi ou avec quelqu'un qui a été victime d'un vol d'identité, vous savez qu'il est extrêmement difficile de réparer les pots cassés. Nous pourrions aider grandement les victimes de ce genre de crime, mais nous sommes loin d'en faire suffisamment.

Voilà ce qui met fin à mes remarques préliminaires. Je suis disposé à répondre à vos questions, que ce soit sur les points que je viens d'aborder ou, évidemment, sur le projet de loi S-4.

La présidente : Merci beaucoup.

Le sénateur Wallace : Je vous félicite pour le travail de précision que vous avez effectué, l'examen exhaustif que vous avez fait sur le sujet, ainsi que les études qui sont affichées en ligne. Nous allons certainement les consulter.

J'ai trouvé intéressant que des banques aient pris part à votre projet. Bien sûr, les banques sont très préoccupées par ce problème, car elles se retrouvent aux premières lignes dans les cas de vol d'identité. Comme le sénateur Dickson l'a souligné plus tôt, quand vous êtes victime d'une fraude par carte de crédit, vous devez être en contact direct avec votre banque. Les établissements bancaires reçoivent les plaintes et doivent composer avec la réalité financière associée à ce genre de crime. Je suis curieux de savoir quelle a été la réaction des banques à l'égard du projet de loi S-4. J'ai discuté avec les représentants de certaines banques, et je me demandais ce que vous pensiez de leur attitude et de l'appui qu'ils témoignent à ce projet de loi.

M. Fewer : Je n'ai entendu aucune critique de la part des banques à propos de ce projet de loi, du moins pas directement, même si je dois avouer que je n'en ai pas discuté personnellement avec des représentants, pas plus que des projets de loi C-27 ou C-299, les projets de loi sur le vol d'identité qui ont précédé celui-ci.

Tamir Israel, stagiaire en droit, Clinique d'intérêt public et de politique d'internet du Canada Samuelson-Glushko : Je ne pense pas que nous ayons consulté les banques à ce sujet.

M. Fewer : Je ne peux donc pas vraiment répondre à votre question.

Permettez-moi de vous présenter Tamir Israel, employé de la CIPPIC. Il a beaucoup travaillé dans le domaine des renseignements confidentiels et personnels et s'intéresse au vol d'identité.

Le sénateur Wallace : Merci. Avez-vous analysé en profondeur ce qui se fait ailleurs dans le monde avant de formuler les nombreuses recommandations qui se trouvent dans votre mémoire? Vous êtes-vous penchés sur la façon dont les autres pays se sont attaqués à la question, et est-ce que ce sont des données sur lesquelles vous fondez l'opinion que vous nous partagez ce matin?

Mr. Fewer: Absolutely. We have done quite a bit of comparative legal research. We are a bit behind the curve in addressing this legislatively. If you look down to the United States in particular, which is a jurisdiction we deal with a great deal and with which we have significant cross-border issues, you see that they are ahead of us in centralizing responses to identity theft issues. The Free Trade Commission, FTC, is kind of the one-stop-shop in the United States for addressing identity theft issues. Also, within states, California in particular has been very progressive in legislating responses to identity theft. We have done a fair amount of work looking at those approaches and comparing them to what we have here in Canada. Bill S-4 goes quite a bit of the way towards adapting many of the approaches in the California law in particular.

Senator Wallace: With many of your recommendations and getting a structure in place and protection in place for citizens, would some of those mechanisms more properly be found outside of the Criminal Code? Has that been your experience in looking at other jurisdictions and how they have dealt with this and having a centralized data repository for some of these issues? Is it fair to say that these should not necessarily all be dealt with within the Criminal Code?

Mr. Fewer: That is absolutely true.

Senator Wallace: Has that been the experience you have seen in other jurisdictions?

Mr. Fewer: Absolutely.

Senator Wallace: Thank you very much. I appreciate that.

Senator Baker: We just heard from a witness prior to you gentlemen who said that the majority of identity theft crime of Canadians actually takes place offshore in other nations. Therefore, if we are passing legislation and it means something, then of course we have to at some point address that problem.

Before I continue, are you the same David Fewer who took the Privacy Commissioner to Federal Court and won on this issue?

Mr. Fewer: Yes.

Senator Baker: Oh, excellent. We passed the PIPEDA law. Within the law, the jurisdiction of PIPEDA was Canada. You took PIPEDA to the Federal Court, section 18.1 of the rules, as a judicial review, and you won. According to my recollection of the judgment, it was only last year or the year before that.

Mr. Fewer: It was not long ago.

Senator Baker: As a result, they now have to investigate this crime in the United States. Could you share with the committee the scheme that you concocted with somebody else to actually initiate this? You went on the Internet and fed somebody's name to an agency that promised to tell you everything you needed to know about this Canadian citizen, their criminal record, their psychological profile and everything, all their personal information. Could you explain to the committee what you did in order to change the law of Canada relating to PIPEDA?

M. Fewer : Absolument. Nous avons mené des travaux de recherche juridique comparative. Nous sommes en retard sur le plan législatif. Par exemple, si on prend les États-Unis, qui est un pays avec lequel nous faisons beaucoup affaire et avons des questions transfrontalières en commun, on constate qu'ils ont une longueur d'avance sur nous et sont mieux en mesure de régler les problèmes de vol d'identité. La Commission du libre-échange est l'institution qui se préoccupe des vols d'identité aux États-Unis. De plus, la Californie s'est montrée particulièrement progressiste en prenant des mesures législatives à cet égard. Nous avons passé beaucoup de temps à examiner ces approches et à les comparer avec celles du Canada. Le projet de loi S-4 a néanmoins adapté bon nombre des approches que l'on retrouve en particulier dans la législation californienne.

Le sénateur Wallace : Compte tenu de vos recommandations visant à mettre en place une structure pour protéger les citoyens, ne serait-il pas préférable que ces mécanismes ne figurent pas uniquement dans le Code criminel? Est-ce ainsi dans les autres pays? Disposent-ils d'un entrepôt de données centralisé pour régler quelques-unes de ces questions? Est-il juste de dire que ces questions ne devraient pas nécessairement toutes relever du Code criminel?

M. Fewer : Tout à fait.

Le sénateur Wallace : Avez-vous observé cela dans d'autres pays?

M. Fewer : Absolument.

Le sénateur Wallace : Merci beaucoup.

Le sénateur Baker : Un des témoins précédents nous a dit que la majorité des vols d'identité dont sont victimes les Canadiens sont commis à l'étranger. Par conséquent, si nous adoptons cette loi et que celle-ci est bien fondée, nous aurons, dans une certaine mesure, remédié au problème.

Avant de poursuivre, êtes-vous le même David Fewer qui a poursuivi la commissaire à la protection de la vie privée devant la Cour fédérale et a obtenu gain de cause?

M. Fewer : Oui.

Le sénateur Baker : D'accord, excellent. Nous avons adopté la LPRPDE. En vertu de la loi, la LPRPDE a une portée canadienne. Vous avez fait une demande de contrôle judiciaire en vertu de l'article 18.1 de la Loi sur les Cours fédérales et vous avez gagné. Si ma mémoire est bonne, cela remonte à un an ou deux.

M. Fewer : Cela ne fait pas longtemps.

Le sénateur Baker : Depuis ce jugement, ce crime fait l'objet d'une enquête aux États-Unis. Pourriez-vous décrire au comité toute votre démarche? Vous êtes allé sur Internet et avez fourni le nom d'un citoyen canadien à un organisme qui vous a promis de vous révéler tout ce que vouliez savoir à son sujet, notamment son dossier criminel, son profil psychologique, et ses renseignements personnels. Pourriez-vous nous dire comment vous vous y êtes pris pour modifier la législation canadienne en ce qui a trait à la LPRPDE?

Mr. Fewer: I would first say that perhaps the honourable senator is overstating the impact of the decision and the argument.

Senator Baker: You would not overstate it.

Senator Campbell: Senator Baker never overstates.

Mr. Fewer: We had a concern in that case that the Privacy Commissioner was effectively fettering herself and effectively restricting the scope of her jurisdiction under the act. It is not that PIPEDA protects Canada; it is that PIPEDA protects Canadians. We urged the commissioner and the court to take a view that the law should protect Canadians in those circumstances where there is a violation of the act in the presence of real and substantial connections to Canada.

In this case, it was basically an information broker who offered a service. I cannot remember the exact name of it, but it was the Canadian information service and had a little Canada flag there as well. It was advertising and saying that if you want to find information out about a Canadian, come to this service and it will give it to you.

Senator Baker: In a foreign nation.

Mr. Fewer: This organization was in the United States, though plainly it had to have agents or conduct investigations in Canada, so there were some connections to Canada. It is difficult to say you are going to investigate a Canadian's telephone records if you are not actually going to in some way engage with a Canadian telephone company. There had to be some connections to Canada, unless the company was just a fraudster, just taking your money and making things up, which, with respect to the psychological reports, may well have been the case.

Senator Baker: They were not right on your psychological report?

Mr. Fewer: I unfortunately did not get one of myself. My former colleague, the former director of the clinic, assures me that her psychological profile was off. I hope it was. Let us put it that way.

Those were the circumstances of the case. It does make it difficult for the Privacy Commissioner to investigate foreign crimes, but this happens all the time in the criminal context and in civil contexts and in other regulatory contexts. We have ample agreements with the United States to basically cooperate with one another on these kinds of investigations. In that particular case, it was not a difficult matter. The FTC had jurisdiction to look into the very same kinds of issues that we were asking the Privacy Commissioner to investigate, and that is what subsequently happened after we got the court decision that said yes, the Privacy Commissioner had jurisdiction. The Privacy Commissioner and the FTC basically cooperated in their investigation. We understand that the FTC will be issuing a finding shortly, and we anticipate it to be something that most Canadian consumers will be happy with.

M. Fewer : Je crois que l'honorable sénateur surestime peut-être l'impact de la décision et des arguments.

Le sénateur Baker : Impossible.

Le sénateur Campbell : Le sénateur Baker n'exagère jamais.

M. Fewer : La commissaire à la protection de la vie privée a mal interprété la portée de ses pouvoirs et était d'avis que la LPRPDE ne lui conférait pas compétence pour mener une enquête. C'est ce qui nous préoccupait. La LPRPDE ne vise pas à protéger le Canada, mais plutôt les Canadiens. Nous avons enjoint la commissaire et le tribunal à s'assurer que la loi protégeait les Canadiens dans les cas de violation, surtout lorsqu'il y a des liens évidents et étroits avec le Canada.

Dans ce cas, c'était un courtier en information qui avait offert le service. Je ne me souviens pas de son nom exact, mais il se présentait comme un service de renseignements canadien et affichait un drapeau du Canada. Il disait pouvoir fournir tous les renseignements dont on avait besoin à propos de n'importe quel Canadien.

Le sénateur Baker : À l'étranger.

M. Fewer : Cette organisation était établie aux États-Unis, mais devait forcément avoir des agents ou des enquêteurs au Canada. Chose certaine, elle entretenait des liens avec le Canada. Il est difficile d'avoir accès aux relevés des appels téléphoniques d'un citoyen canadien sans faire affaire avec une compagnie de téléphone canadienne. L'entreprise doit nécessairement avoir des liens avec le Canada, à moins de n'être qu'un fraudeur qui vous soutire de l'argent et invente n'importe quoi, par exemple, sur votre profil psychologique.

Le sénateur Baker : On s'est trompé sur votre profil psychologique?

M. Fewer : Je n'ai malheureusement pas été évalué. Mon ancien collègue, l'ancien directeur de la clinique, m'a assuré que son profil ne correspondait pas du tout. Du moins, je l'espère.

Ce sont donc les circonstances entourant l'affaire. Il est difficile pour la commissaire à la protection de la vie privée d'enquêter sur des crimes à l'étranger, mais cela arrive tout le temps dans les contextes criminel, civil et réglementaire. Nous nous sommes entendus avec les États-Unis pour collaborer dans ce genre d'enquêtes. Dans ce cas, ce n'était pas difficile. La Commission de libre-échange a compétence pour faire enquête sur les questions que nous voulions que la commissaire examine; par conséquent, ceux-ci ont pu collaborer lorsque la Cour a statué que la commissaire à la protection de la vie privée avait aussi compétence. Nous savons que la commission publiera bientôt ses conclusions, et nous pensons que les Canadiens en seront satisfaits.

Senator Baker: We congratulate you on your success in extending the jurisdiction of the Privacy Commissioner of Canada to the collection of identify theft material in the United States and in a foreign jurisdiction. It was a marvellous case.

In this particular bill, you praised the question of damages. That is, when the sentence is being given, an award shall be given, as I understand the wording, relating to damages suffered because of the identity theft. In your submission, you say that collecting damages is a costly venture. Under PIPEDA and our Privacy Act, directly in the act, an application to the Federal Court for damages is allowed.

Now we have in the legislation, together with another piece of legislation under PIPEDA, two routes to go for compensation, and the cost involved with going to the Federal Court. However, do you still think that what is in this legislation takes precedence over what is already on the books?

Mr. Fewer: This is better than what PIPEDA has to offer, absolutely.

Senator Milne: When I was first appointed to the Senate in another committee at another time, we heard evidence from one of these information collectors in the United States that they could, if you wanted, provide for a fee the name and address of every single left-handed fly fisher in the United States. That is how much information they have collected about every single person. It is absolutely incredible. I congratulate you.

Senator Campbell: Mr. Fewer, you should know that it is rare that the Svengali of case law in this committee, Senator Baker, genuflects, but I did see a slight motion on his part, so you should be quite honoured by that.

My simple question has to do with the police report. If you are involved in an investigation and you make a police report, you will get a case number from the police. If you ever need to refer to that for whatever reason, it would simply be a matter of giving them the case number and that could be confirmed.

Why is it so important to get the police report? Regarding the difficulties involved in a police report because of the Privacy Act, you will get a police report but it will be black except for the words ''a'' and ''the.'' Everything else will be blacked out except, perhaps, your name. Why would the case number alone not be sufficient?

Mr. Fewer: In our more detailed comments, we think that the police report will help streamline the process by which victims will be able to remove fraudulent activity from their various records — financial, criminal, medical, and so forth. That streamlined process would also assist consumer reporting agencies, businesses, collection agencies and others who need to deal with the consequences of identity fraud.

Le sénateur Baker : Nous vous félicitons d'avoir réussi à étendre les pouvoirs de la commissaire à la protection de la vie privée lui permettant de recueillir des renseignements aux États-Unis et ailleurs à l'étranger dans le cadre d'une enquête. C'était un cas merveilleux.

En ce qui concerne le présent projet de loi, vous avez appuyé la disposition prévoyant le paiement de dommages-intérêts. Lorsqu'une peine est imposée, une indemnisation serait accordée aux victimes de vol d'identité, si je comprends bien, en fonction des dommages causés. Dans votre mémoire, vous dites que de tels litiges sont coûteux. Aux termes de la LPRPDE et de la Loi sur la protection des renseignements personnels, dans le cas de dommages, on peut présenter une demande à la Cour fédérale.

En vertu du projet de loi et de la LPRPDE, nous avons maintenant deux voies de recours pour obtenir une indemnisation relativement aux dommages et aux coûts liés aux poursuites devant la Cour fédérale. Cependant, êtes-vous toujours d'avis que les dispositions de cette mesure législative ont préséance sur les dispositions existantes?

M. Fewer : Absolument. Cela surpasse certainement ce que la LPRPDE a à offrir.

Le sénateur Milne : Lorsque j'ai été nommée pour la première fois au Sénat, des courtiers en information des États-Unis ont comparu devant un autre comité et ont indiqué qu'ils pouvaient, moyennant de l'argent, nous fournir le nom et l'adresse de tous les moucheurs gauchers des États-Unis. Ils sont capables de tout savoir sur une personne. C'est absolument incroyable. Je vous félicite.

Le sénateur Campbell : Monsieur Fewer, sachez qu'il est rare que le Svengali de la jurisprudence au sein de ce comité, le sénateur Baker, s'incline, mais j'ai vu un léger mouvement de sa part, alors vous devriez en être honoré.

Ma question porte sur le rapport de police. Si vous faites l'objet d'une enquête et, par le fait même, d'un rapport de la police, on vous donnera un n^{o} de dossier auquel vous référer. Par conséquent, si vous voulez obtenir une copie du rapport, il vous suffit de fournir ce n^{o}.

Pourquoi est-il si important de pouvoir avoir accès à ce rapport de police? En vertu de la Loi sur la protection des renseignements personnels, vous recevrez une copie, mais elle sera en grande partie masquée. Tout sera censuré, à l'exception peut-être de votre nom. Pourquoi le n^{o} de dossier ne serait-il pas suffisant?

M. Fewer : Nous pensons que le rapport de police permettra de simplifier le processus, de sorte que les consommateurs seront mieux à même de protéger leurs dossiers — financiers, criminels, médicaux, et cetera — contre la fraude. Ce processus simplifié pourrait également aider les agences de renseignements sur les consommateurs, les entreprises et les agences de recouvrement, entre autres, qui doivent composer avec les conséquences du vol d'identité.

The report is more than just a number. To a certain extent, the report is an authenticated, trustworthy document, something that businesses can rely upon and use to make better decisions about how to respond to remediation requests.

Senator Campbell: It will not tell you anything. If you have seen a police report after you have asked for one, it will not tell you anything. At the end of the day, it will just be a blacked out document with your name, date, address and phone number. That is what I am saying.

I understand why you would want something that says, ''I am innocent; my name is clean.'' However, I do not see how the police report would do that, nor do I see that that is the responsibility of the police. You could be waiting years for that final police report to be concluded. I understand the need for that. If you are in a situation where each time you use your credit card, someone says, ''Oh, sorry,'' and you have to then phone and say, ''No, it was not me,'' I do not think the police report will get that for you.

You did a great job on the rest of it.

Senator Joyal: Mr. Fewer, I believe we have a phenomenon that we have not addressed specifically. It is the following: Companies have been building information on individuals through recoupment of all kinds of sources, and then they sell that information. We will have more of that because it is becoming a marketing tool. If you want to sell blue-rimmed glasses, a company will tell you to which customer you should offer blue-rimmed glasses on the basis of the information that they have compiled in data banks.

There is a free market of information. It is a free business. Anyone can compile information about anybody and sell it. At the same time, we have not defined the responsibility of those companies to ensure that they do not break into that information and use it for creating or stealing identities.

If we want to show the public that we are aware of what is going on, we have to be aware that this is the reality now. You have studied it better than any of us here around the table.

We are concerned about addressing the specific case of somebody who steals a passport and pretends to be the other person. That is the easy thing, and I believe there are now a small number of cases. That is not where the problem lies in terms of volume.

There is more volume in breaking into a computer where all kinds of data are stored, or in being connected to eBay and being able to hack the credit cards of people who buy on eBay. Any one of us knows stories like that. My assistant who buys on eBay has told me his credit card has been used fraudulently three times.

Those are the kinds of problems we have. It is not enough just to tell companies that they have to be prudent and they have to work with the police. There must be a new responsibility there.

Le rapport est plus qu'un n°. Dans une certaine mesure, le rapport est un document authentifié et fiable sur lequel les entreprises peuvent se fonder pour prendre de meilleures décisions quant aux mesures correctives.

Le sénateur Campbell : Il ne nous dit pas grand-chose. Si vous demandez un rapport de police, vous verrez qu'il ne vous apprendra rien. Vous vous retrouverez avec un document noirci contenant la date ainsi que votre nom, adresse et n° de téléphone.

Je comprends la nécessité d'avoir un document qui confirme votre innocence; cependant, je ne vois pas comment le rapport de police pourrait le faire ni en quoi cela relève de la responsabilité de la police. Vous pourriez attendre plusieurs années avant qu'un rapport de police ne soit conclu. Toutefois, je comprends ce que vous dites, particulièrement si vous devez clamer votre innocence chaque fois que vous utilisez votre carte de crédit. Par contre, je ne crois pas que le rapport de police pourrait y changer quoi que ce soit.

Vous avez fait un travail remarquable sur les autres aspects.

Le sénateur Joyal : Monsieur Fewer, je pense que nous assistons à un phénomène dont nous n'avons pas encore discuté. Les entreprises recueillent de l'information sur des gens à partir de diverses sources, puis vendent cette information. C'est un phénomène grandissant et c'est devenu un outil de commercialisation. Si vous vendez des lunettes à montures bleues, la compagnie vous dira à qui vous adresser selon les données qu'elle a compilées.

C'est un libre marché de l'information. Tout le monde peut recueillir des renseignements sur n'importe qui, puis les vendre. En même temps, nous n'avons pas défini la responsabilité de ces entreprises afin de nous assurer qu'elles n'utilisaient pas ces données pour créer ou voler des identités.

Si nous voulons démontrer au public que nous savons ce qui se passe, nous devons reconnaître que c'est une réalité. Vous avez étudié la question plus que quiconque autour de cette table.

Nous voulons régler le cas des gens qui volent un passeport et se font ensuite passer pour la personne. C'est facile à faire, et je pense qu'il y a maintenant un petit nombre de cas. Ce n'est pas le plus gros problème en termes de volume.

Il y a beaucoup plus de cas de pirates informatiques qui entrent dans des bases de données et des réseaux pour commettre des fraudes avec les cartes de crédit des gens qui achètent sur eBay. Nous avons tous déjà entendu des histoires à ce sujet. Mon adjoint, qui effectue des achats sur ce site Web, m'a dit que sa carte de crédit a été utilisée de manière frauduleuse à trois reprises.

Ce sont les types de problèmes auxquels nous sommes confrontés. Il ne suffit pas de dire aux compagnies de faire preuve de prudence et de collaborer avec la police. Elles doivent assumer une nouvelle responsabilité.

As much as this bill has objectives to which all of us ascribe, I have the perception that we will remain short of what will come and develop in the years to come.

I am supportive of the bill, as you are, and as some other witnesses have been. However, as you know, it is very difficult to have legislation passed in Parliament and have it adjusted later on. In this legislation, especially, there is no obligation on Parliament to review it after a while to ensure that it still meets the objectives. Therefore, we should be concerned with trying to deal with the problem that is emerging through the way the system develops.

You alluded to it in your brief when you mentioned the data protection law and so forth. As you said quite clearly, this problem is not addressed in the legislation.

Mr. Fewer: I would agree with everything that you have said. This legislation is good for what it does. It should not even pretend to be a comprehensive attempt to address identity theft issues. The security breach side, when an organization that collects and uses personal information then does not use appropriate safeguards or does use safeguards or uses inadequate safeguards or has breached through no fault of its own, is a problem. That harm has been known for some time. I would take the government to task a little bit for not having introduced data-breach legislation at this point. I understand the issues are a little difficult, but the problem has been identified and we need to move forward to address it.

Senator Joyal: It seems to me that this is a key issue with the way the technology is evolving. The worst of the scenarios is that those data banks are stored somewhere other than in Canada. It is so easy for the information to travel around the world. If I were an ill-intentioned person, I would never establish my working base in a country where there is legislation; I would go to countries where the legislation is more lax. If you say the United States has better legislation, I would go somewhere else. I will not name any countries. I do not want to offend anyone.

We know, for instance, that today the information centres for many Canadian companies are located in Asia and around the world. It is easy for someone who wants to break into those data banks to do it, especially if they operate from countries where the legal system and the police are more lax than ours.

It is not as if the guy we are trying to find is across the street or in the neighbouring town. The people we sometimes want to find are located thousands of kilometres away. It seems to me that we should be concerned about reflecting that reality, and we know that it will be emerging and developing in the future.

I am not sure that this bill, as much as it is good, is just the preliminary of what should be our comprehensive approach to fighting Internet crime, generally speaking, which is linked to what we want to achieve because most of that stolen information is stolen through the Internet. The largest number of cases comes through the Internet.

Autant que ce projet de loi vise des objectifs auxquels nous souscrivons tous, j'ai l'impression que nous n'arriverons pas à suivre les développements dans les années à venir.

Tout comme vous et d'autres témoins, je suis en faveur de ce projet de loi. Toutefois, comme vous le savez, il est très difficile d'adopter une loi au Parlement, puis de l'ajuster plus tard. Dans le cas de ce projet de loi en particulier, le Parlement n'est nullement tenu de le réviser après un certain temps, puis de s'assurer qu'il atteint ses objectifs. Par conséquent, nous devrions nous employer à régler un problème de plus en plus présent en raison de l'évolution du système.

Vous y avez fait allusion dans votre mémoire lorsque vous avez parlé de la Loi sur la protection des renseignements personnels et ainsi de suite. Comme vous l'avez dit clairement, ce projet de loi ne tient aucunement compte de ce problème.

M. Fewer : Je suis entièrement d'accord avec vous. Ce projet de loi accomplit certaines choses, mais on ne devrait pas prétendre qu'il s'agit de la solution au problème des vols d'identité. Lorsqu'une organisation qui recueille et utilise des renseignements personnels n'a pas en place des mécanismes de protection adéquats ou viole involontairement la confidentialité de l'information, il y a atteinte à la sécurité. Cette situation a été mise au jour il y a un certain temps déjà. Je reproche au gouvernement de ne pas avoir pris des mesures législatives à ce chapitre. Je suis conscient que ce sont des questions difficiles, mais on a cerné le problème. Il ne reste plus qu'à s'y attaquer.

Le sénateur Joyal : Il me semble que c'est une question clé, compte tenu de l'évolution de la technologie. Des données entreposées à l'étranger représentent le pire des scénarios. L'information circule si facilement à travers le monde. Si j'étais une personne mal intentionnée, je ne m'établirais jamais dans un pays où il y a des lois à cet égard, mais plutôt dans un pays où les lois sont beaucoup plus souples. Si vous dites que les États-Unis ont adopté les meilleures lois, j'irais ailleurs. Je ne nommerai personne. Je ne voudrais pas offenser qui que ce soit.

Nous savons, par exemple, qu'aujourd'hui, les centres d'information de nombreuses entreprises canadiennes se trouvent en Asie et partout dans le monde. Il est donc facile pour une personne d'accéder à ces banques de données, particulièrement si elles se trouvent dans un pays où le système juridique et la police sont beaucoup moins rigoureux qu'ici.

Ce n'est pas comme si la personne que nous cherchions se trouvait de l'autre côté de la rue ou dans le quartier avoisinant. Il est souvent question de milliers de kilomètres. Il me semble que nous devrions nous soucier de refléter la réalité, car nous savons que cette situation prendra de l'ampleur dans le futur.

Bien qu'il s'agisse d'un bon projet de loi, je ne crois pas qu'il nous permette de lutter contre les cybercrimes en général. Il faut y accorder une certaine importance, puisque la plupart des renseignements sont volés à partir d'Internet.

Mr. Fewer: That point goes back to a point raised earlier about the limitations of criminal law for addressing all of these aspects. Spyware, spam, phishing and pharming are all exotic names for new Internet crimes. All of these behaviours have international components to them. To a certain extent, the international community is doing a reasonable job of coordinating on some of these issues. However, much more could be done. I would agree that a final solution to these problems requires an international cooperation, public-private partnerships and both criminal and regulatory responses.

Senator Joyal: On page 3 of your brief you mention that clause 11 of the bill provides for restitution to victims of identity theft, and you make two recommendations after having commented that the benefits of the restitution for victims are minimal in clause 11. You recommended in your conclusion, in the fourth bullet on page 8, two additional provisions to the Criminal Code: "Adding provisions within the Criminal Code granting victims of identity crimes a right to a local police report and a right to a judicial order of innocence."

Since you are a jurist, could you explain more about how you would phrase that in the Criminal Code?

Mr. Fewer: My quick response is to look at California again. My suggestion for both the police report and for the court order comes from California legislation that consumer advocates have found to be helpful. I do not have a copy of the legislation in front of me. Do you have it, Mr. Israel?

The Chair: If you could even give us the name of the relevant act we can probably find it on the Internet and I will ask our researchers to do that.

Senator Joyal: Not in a data bank.

The Chair: No; nor with any of our names attached.

Mr. Fewer: I do not have it on hand immediately, but I will undertake to provide it to the clerk following this and she can forward it to the members.

The Chair: That would be appreciated.

Senator Joyal: On the other issue of the crime of breaking into a data bank, could you provide us with comparative legislation that you might have at hand so that we could reflect upon the need to have a similar provision or comparable provision in the code, considering that this is one of the key elements of crimes related to identity theft and other related crimes?

You advocate the creation of a national identity theft victim resource and assistance bureau. Do you see that as a national institution? Could you explain in larger terms what you mean by that?

M. Fewer : Cela revient à ce qui a été dit plus tôt à propos des limites du droit pénal. Les logiciels espions, les pourriels, l'hameçonnage et le détournement de domaine font tous partie des nouveaux crimes perpétrés sur Internet. Toutes ces infractions ont une composante internationale. Dans une certaine mesure, la communauté internationale s'acquitte raisonnablement bien de ses tâches en gérant quelques-unes de ces questions. Toutefois, il reste encore beaucoup de chemin à faire. Pour remédier à ces problèmes une fois pour toutes, je conviens qu'il faut miser sur la collaboration internationale, des partenariats entres les secteurs public et privé et des mesures pénales et réglementaires.

Le sénateur Joyal : À la page 3 de votre mémoire, vous mentionnez l'article 11 du projet de loi qui prévoit un paiement de dommages-intérêts aux victimes de vol d'identité — avantages d'indemnisation que vous qualifiez de minimes —, puis vous faites deux recommandations à cet égard. Dans votre conclusion, au quatrième point à la page 10, vous recommandez deux dispositions supplémentaires au Code criminel : « Ajouter au Code criminel des dispositions accordant aux victimes de crimes liés à l'identité le droit à un rapport de la police locale et à une déclaration judiciaire d'innocence. »

Comme vous êtes un homme de loi, pourriez-vous nous expliquer plus en détail comment vous formuleriez ces dispositions dans le Code criminel?

M. Fewer : Ma réponse, en quelques mots, c'est de prendre l'exemple de la Californie encore une fois. Ma recommandation en ce qui concerne le rapport de police et l'ordonnance de tribunal s'inspire de la législation californienne, et les groupes de défense des consommateurs la trouvent également utile. Je n'ai pas d'exemplaire à portée de la main. L'avez-vous, monsieur Israel?

La présidente : Si vous pouviez nous trouver le nom de la loi pertinente, nous pourrions probablement la trouver sur Internet, et je demanderais à nos attachés de recherche de s'en occuper.

Le sénateur Joyal : Pas dans une banque de données.

La présidente : Non, pas plus qu'avec n'importe quel nom que nous donnons.

M. Fewer : Je n'ai pas d'exemplaire avec moi, mais je le ferai parvenir à la greffière après la séance, et elle pourra le distribuer aux membres.

La présidente : Ce serait bien aimable.

Le sénateur Joyal : En ce qui a trait à l'autre type de crime, à savoir l'entrée par effraction dans une banque de données, avez-vous en main une mesure législative comparable à nous donner pour que nous puissions réfléchir à la nécessité d'avoir une disposition semblable ou comparable dans le Code, étant donné que c'est l'un des principaux éléments des crimes liés au vol d'identité et à d'autres crimes connexes?

Vous préconisez la création d'un bureau national d'information et d'aide aux victimes de vol d'identité. Envisagez-vous d'établir une institution nationale? Pouvez-vous nous expliquer davantage ce que vous entendez par là?

Mr. Fewer: The issue is that identity theft is a crime that keeps victimizing the victim over and over — every time you go to get a new credit card or you apply for a loan for your house, or if you are just doing nothing and you find out that, again, your documents have been used to commit some further fraud. The question is how we can help victims in this space. It turns out it is incredibly difficult for victims to remediate, to clear their name, to put a stop to continuing frauds. You have to go from institution to institution. At each institution you may have to educate anew because you are dealing with someone at the help desk who has never had to deal with an identity theft issue before. That person does not understand. He or she suspects that you are a fraudster and again you are victimized.

Our view is that this crime is becoming common enough and is harmful enough to justify putting some public resources towards helping victims clear their names and prevent further frauds from occurring. It makes sense to do it nationally because so many of our institutions are national. It makes sense as well not to have to duplicate resources. Even for institutions that are not national the issues are still the same. Regardless of where your bank is or where your credit card is issued from, the issues will arise in the same way, and it would be very helpful to consumers if they had a resource that could basically take them by the hand and take them through the process of remediating and clearing their name and clearing the fraud.

Senator Joyal: How do you see that office or registry being financed? Do you see that through contributions from credit card companies or banks or financial institutions that provide or will collect that information?

Mr. Fewer: To be frank, I would like to see the institution arise. As to how it is funded, I am very flexible. It could very well be funded through organizations that would benefit from that institution; banks, credit card companies, mortgage lenders, those kinds of institutions.

It may be the kind of thing that we characterize as an investment. Such an institution certainly could have the mandate of remediation, but it could also have the mandate of consumer education, helping consumers understand how to prevent such crimes from arising in the first place. It could also help organizations with security breach issues, helping them understand how they could prevent such crimes from happening in the first place.

The Chair: On a supplementary, are you familiar with a federal-provincial body, which does exist, called the Consumer Measures Committee?

Mr. Fewer: I am.

The Chair: What you are talking about, at least part of it, sounds a lot like what I understand to be their mandate, including doing research and analysis and developing consumer education initiatives.

Mr. Fewer: My understanding of the CMC is that it does not have a desk. There is no place I can go to and say, "I am a consumer and I have a problem." It is not a complaints

M. Fewer : Le problème avec le vol d'identité, c'est qu'il s'agit d'un crime où la victime ne cesse d'être victimisée — chaque fois qu'on se procure une nouvelle carte de crédit ou qu'on fait une demande de prêt hypothécaire, et même si on ne fait rien, on peut découvrir, une fois de plus, que nos documents ont été utilisés pour commettre d'autres fraudes. La question est de savoir comment aider les victimes dans ce contexte. En fait, les victimes ont beaucoup de mal à rétablir leur identité, à se disculper et à mettre un terme aux fraudes continues. Vous devez passer d'une institution à l'autre et, chaque fois, présenter votre cas à nouveau parce que le préposé n'a jamais eu à traiter un dossier de vol d'identité auparavant. Il ne comprend pas. Même qu'il vous soupçonne d'être le fraudeur et, une fois de plus, vous voilà victimisé.

Selon nous, ce crime est suffisamment fréquent et nuisible pour justifier l'attribution de ressources publiques en vue d'aider les victimes à se disculper et à prévenir d'autres fraudes. Il est logique de le faire à l'échelle du pays parce que bon nombre de nos institutions sont nationales. Il est également logique de ne pas faire un double emploi des ressources. Même pour les institutions qui ne sont pas nationales, les enjeux restent les mêmes. Peu importe où se trouve votre banque ou d'où votre carte de crédit est émise, les problèmes surgiront de la même manière; il serait donc très utile pour les consommateurs de pouvoir compter sur une ressource qui les épaulerait tout au long du processus de réparation et de disculpation.

Le sénateur Joyal : Comment ce bureau ou ce registre sera-t-il financé, selon vous? Serait-ce par l'entremise de contributions des compagnies de carte de crédit ou des banques ou des institutions financières qui fournissent ou recueillent cette information?

M. Fewer : Pour être honnête, je tiens à ce que l'institution soit établie. Quant à savoir comment la financer, je suis très ouvert. Elle pourrait très bien être financée par l'entremise d'organisations qui en bénéficieraient : les banques, les compagnies de carte de crédit, les prêteurs hypothécaires et d'autres institutions de ce genre.

C'est ce que nous pourrions qualifier d'investissement. Une telle institution pourrait certes avoir pour mandat de remédier au tort causé, mais on pourrait également lui confier le mandat de sensibiliser les consommateurs et de les aider à comprendre comment prévenir ces crimes en premier lieu. Elle pourrait également aider des organisations aux prises avec des problèmes d'atteinte à la sécurité, en leur montrant comment s'y prendre pour empêcher que de tels crimes se produisent.

La présidente : Juste en passant, êtes-vous au courant d'un organisme fédéral-provincial appelé le Comité des mesures en matière de consommation?

M. Fewer : Oui.

La présidente : Ce dont vous parlez, du moins en partie, ressemble beaucoup au mandat de cet organisme, d'après ce que je comprends, notamment la recherche, l'analyse et l'élaboration d'initiatives en matière de sensibilisation des consommateurs.

M. Fewer : À ma connaissance, le CMC n'a pas de bureau. Il n'y a pas d'endroit où je peux me présenter et dire : « Je suis un consommateur et j'ai un problème. » Il ne s'agit pas d'une

organization or a consumer-assistance organization. It operates at a higher level. It is an excellent organization. As a consumer advocate, I would love to see its mandate expanded and its reach lengthened. That may be an appropriate venue for this kind of initiative.

There are other appropriate venues as well. This is not far off from what the Privacy Commissioner does. The Competition Bureau similarly takes complaints from the consumer, although they do not often have a consumer-assistance mandate. The Canadian Radio-television and Telecommunications Commission, CRTC, to a certain extent also takes complaints. Through the CRTC, we now have the do-not-call registry, which is a much more consumer-facing issue. The CRTC also oversees the implementation of the telecommunications complaints ombudsperson, which is another consumer-facing bureau. All of these institutions have some problems. None is quite the institution we have in mind for this.

Senator Joyal: As I was listening to the witnesses, it occurred to me there is a principle that inasmuch as data banks develop, someone holds them as they continually grow. At some point in time, the responsibility of that person must be called into action because the risk is bigger as a result of the amount of data involved. There must be a signal somewhere that you can do this, but you must take additional measures and initiatives to be sure that the banks are protected. In addition, you share the responsibility if there is a break-in at some point in time and you must be part of the compensation scheme.

I see more the system as a whole than trying to pinch one element or pinch another element, running after amending sections of the code each time a new problem arises. It seems to me that we have to have an approach that is comprehensive in how reality operates today.

Mr. Fewer: I would agree. I would not want you to leave this meeting thinking that our position is that the consumer should be absolved of all responsibility. This is true in almost every area of harmful Internet behaviour that we look at, such as spam, spyware, phishing or pharming. Consumers must take responsibility for their actions.

To a certain extent, however, we must be reasonable in that call. Consumers need to be informed of the risks associated with what they are doing. We think that most businesses have incentives not to be as forthright or upright as they could be in disclosing the risks associated with entering into transactions with them. I say that for two reasons. First, it might scare some consumers off from doing business. Second, on the back side, if businesses do something wrong, what harm is there? In other

organisation de traitement des plaintes ou d'une organisation d'aide aux consommateurs. Elle fonctionne à un niveau supérieur. C'est une excellente organisation, soit dit en passant. En tant que défenseur des intérêts des consommateurs, je serais ravi de voir son mandat élargi et son rayonnement étendu. Elle pourrait convenir à ce genre d'initiative.

Mais il y a d'autres solutions. Ce n'est pas loin du mandat de la commissaire à la protection de la vie privée. Le Bureau de la concurrence s'occupe également des plaintes déposées par les consommateurs, même si, dans bien des cas, il n'a pas pour mandat d'aider les consommateurs. Le Conseil de la radiodiffusion et des télécommunications canadiennes, le CRTC, dans une certaine mesure, traite également des plaintes. Dans le cadre du CRTC, nous avons maintenant le registre des abonnés auto-exclus, qui rejoint davantage les consommateurs. Le CRTC supervise aussi la mise en œuvre du bureau de l'ombudsman pour les plaintes relatives aux télécommunications, qui est un autre bureau d'aide aux consommateurs. Toutes ces institutions posent des problèmes. Elles ne rivalisent pas tout à fait celle que nous avons en tête.

Le sénateur Joyal : Pendant que j'écoutais les témoins, j'ai pensé à un principe : à mesure que les banques de données se développent, quelqu'un est là pour s'en occuper. À un moment ou à un autre, cette personne sera appelée à intervenir parce que le risque deviendra de plus en plus important à cause de la quantité de données en cause. Il faut un signe, quelque part, qui nous indique quand intervenir, mais on doit prendre des mesures et des initiatives supplémentaires pour être sûr que les banques sont protégées. De plus, comme on partage la responsabilité, s'il y a une atteinte à la sécurité à un moment donné, on doit faire partie du régime d'indemnisation.

Je conçois davantage le système comme un tout plutôt que d'essayer d'insérer des éléments ici et là et de modifier des articles du code chaque fois qu'un nouveau problème survient. Nous devons adopter, me semble-t-il, une approche globale qui correspond à la réalité d'aujourd'hui.

M. Fewer : Je serais d'accord. Je ne voudrais pas que vous sortiez de la réunion en pensant que notre position consiste à dire que le consommateur doit être déchargé de toute responsabilité. Cela vaut pour presque chaque catégorie de comportement préjudiciable sur Internet que nous examinons, comme le pourriel, les logiciels espions, l'hameçonnage ou le détournement de domaine. Les consommateurs doivent assumer la responsabilité de leurs actes.

Toutefois, à plusieurs égards, nous devons être raisonnables. Les consommateurs doivent être mis au courant des risques associés à ce qu'ils font. Nous pensons que la plupart des entreprises ont des incitatifs pour ne pas être aussi directes qu'elles ne pourraient l'être au moment de communiquer les risques associés aux transactions. Je dis cela pour deux raisons. Premièrement, cela pourrait dissuader les consommateurs de faire des affaires. Deuxièmement, d'un autre côté, si les entreprises font quelque chose de pas correct, quel mal

words, if they breach their obligations often and disclose to consumers about the nature of the information they collect, how they use it and to whom they disclose it, what is the penalty?

You have seen in our brief, and we have articulated consistently before other legislative committees, the need for better enforcement of our privacy laws against organizations that collect, use and disclose personal information. We think if there were better enforcement on the back side, there would be better consumer information on the front side, which would lead to a reduction of harms.

The Chair: Senator Joyal put at least two of the questions that were troubling me, so I thank him for that.

There is one further question I would like to ask. You are concerned about the need for people to be notified when there has been a security breach or when their identity has been stolen in whole or in part. You suggest that be done in federal privacy laws. The bill before us affects the Criminal Code, and I take it that you do not think that requirements for notification of security breaches belong in the Criminal Code.

Mr. Fewer: No.

The Chair: Why not?

Mr. Fewer: No, I do not believe they do because the kind of behaviour we are talking about here, the kind of fault we are talking about is regulatory or civil; it does not belong in the Criminal Code. We have a fairly comprehensive code to address commercial dealings with personal information of Canadians, and that is under PIPEDA.

The security breach issue strikes me as a gaping hole in what is otherwise a comprehensive regulatory approach to personal information, so it is best addressed there.

The Chair: This came up last night in our hearings, and I was puzzled as to why it might not perhaps, in addition, be addressed in the Criminal Code because of the immense damage that can be suffered by someone who is unaware that their identity has been stolen.

Therefore, if someone, your bank or some institution, knows that that identity has been stolen and that the person is at risk of great damage, failure to notify — I do not want to use the word "criminal" because that is technical and it pre-judges the answer — but it is such an immensely offensive and damaging act that I wonder where the dividing line would be to say this is or is not criminal.

Mr. Fewer: That is an interesting approach. Keep in mind we are talking about commercial behaviour, commercial entities engaging in applying business judgments to their dealings with personal information. We usually reserve criminal law for those

y a-t-il là-dedans? Autrement dit, si elles manquent souvent à leurs obligations et qu'elles divulguent aux consommateurs la nature des données qu'elles recueillent, les fins pour lesquelles elles les utilisent et à qui elles les communiquent, quelle en serait la pénalité?

Comme vous l'avez vu dans notre mémoire, et nous l'avons dit invariablement devant d'autres comités législatifs, il faut une meilleure application de nos lois sur la protection de la vie privée afin de protéger les consommateurs contre des organisations qui recueillent, utilisent et communiquent des renseignements personnels. Selon nous, s'il y a une meilleure application de loi, en aval, il y aura de meilleures informations mises à la disposition des consommateurs, en amont, ce qui réduirait les dommages.

La présidente : Le sénateur Joyal a posé au moins deux des questions qui m'intéressaient, donc je l'en remercie.

Il y a une autre question que j'aimerais vous poser. Vous avez des réserves à l'égard de l'exigence d'aviser les gens en cas d'atteinte à la sécurité ou en cas de vol de leur identité, en tout ou en partie. Vous recommandez de recourir à des lois fédérales en matière de protection des renseignements personnels. Le projet dont nous sommes saisis touche le Code criminel, et je présume que vous ne pensez pas que les exigences de notification des atteintes à la sécurité relèvent du Code criminel.

M. Fewer : En effet.

La présidente : Pourquoi?

M. Fewer : Je ne pense pas qu'elles relèvent du code parce que le genre de comportement ou de faute dont il est question ici est de nature réglementaire ou civile; ces dispositions n'ont pas leur place dans le Code criminel. Nous disposons d'un code assez détaillé pour protéger les renseignements personnels des Canadiens dans les transactions commerciales : la LPRPDE.

Je considère la question de l'atteinte à la sécurité comme un trou béant dans ce qui constitue autrement une approche réglementaire détaillée en matière de protection des renseignements personnels. C'est pourquoi cette question est mieux traitée là-dedans.

La présidente : On a soulevé cette question hier soir, durant nos audiences, et je ne comprenais pas trop pourquoi elle ne pourrait pas être traitée tout aussi bien dans le Code criminel puisque cela cause un tort immense à la personne qui ignore que son identité est volée.

Par conséquent, si une personne, votre banque ou une institution quelconque, sait que votre identité est volée et que la victime court un risque important de préjudice, le fait de ne pas le signaler — et je n'ose pas utiliser le terme « criminel » parce que c'est technique et cela porte un jugement avant même de fournir une réponse —, mais il s'agit d'un geste si offensant et préjudiciable que je me demande où se trouve la ligne de démarcation entre ce qui est criminel et ce qui ne l'est pas.

M. Fewer : C'est une approche intéressante. N'oubliez pas qu'on parle d'un comportement dans un contexte commercial, c'est-à-dire des entités commerciales qui portent des jugements d'affaires dans leur utilisation des renseignements personnels.

most extreme violations of the public trust, especially in the commercial setting, such as the Enrons and the deliberate polluters, these kinds of things.

Where it is a case of negligence, I query whether that rises to the level that we want to be putting our public criminal resources towards it. Thankfully, I do not think we have had to deal with issues of commercial entities going beyond negligence so that they are deliberately putting consumers in jeopardy. If organizations are involved to that degree of malfeasance with respect to personal information, usually they are up to other things that are no good.

The Chair: You can get them some other way?

Mr. Fewer: We can catch them under fraud, counterfeiting or some other bad behaviour, yes.

The Chair: Thank you very much. Thank you to both our witnesses. You have been very helpful and very interesting. We will bear in mind your various representations as we go forward.

Our next meeting will be on Wednesday, May 27, in this room at 4 p.m. or when the Senate rises.

(The committee adjourned.)

Nous réservons le droit criminel habituellement à ceux qui trahissent au plus haut point la confiance du public, surtout dans un cadre commercial, comme les sociétés de type Enron et les pollueurs délibérés, et cetera.

S'il s'agit d'un cas de négligence, je me demande si cela justifierait qu'on y consacre des ressources publiques du régime pénal. Heureusement, je ne pense pas que nous ayons eu des cas où des entités commerciales étaient si négligentes qu'elles ont délibérément causé du tort aux consommateurs. Si des organisations participent à ce degré de malfaisance relativement aux renseignements personnels, il y a fort à parier qu'elles font d'autres choses qui ne sont pas correctes.

La présidente : Pouvons-nous les attraper d'une autre manière?

M. Fewer : Oui, nous le pouvons, dans le cadre des infractions de fraude, de contrefaçon ou d'un autre comportement déloyal.

La présidente : Merci beaucoup. Je remercie nos deux témoins. Vous avez fait des observations très utiles et très intéressantes. Nous en tiendrons compte tout au long de nos travaux.

Notre prochaine réunion aura lieu le mercredi 27 mai, dans la même salle, à 16 heures ou quand le Sénat lèvera la séance.

(La séance est levée.)

APPEARING

Wednesday, May 13, 2009

The Honourable Rob Nicholson, P.C., M.P., Minister of Justice and Attorney General of Canada.

WITNESSES

Wednesday, May 13, 2009

Department of Justice Canada:

Joanne Klineberg, Counsel, Criminal Law Policy Section.

Thursday, May 14, 2009

Information Technology Association of Canada:

David McMahon, Advisor, National Security — Bell Canada.

Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic:

David Fewer, Acting Director;

Tamir Israel, Articling student.

COMPARAÎT

Le mercredi 13 mai 2009

L'honorable Rob Nicholson, C.P., député, ministre de la Justice et procureur général du Canada.

TÉMOINS

Le mercredi 13 mai 2009

Ministère de la Justice Canada:

Joanne Klineberg, avocate, Section de la politique en matière de droit pénal.

Le jeudi 14 mai 2009

Association canadienne de la technologie de l'information:

David McMahon, conseiller, Sécurité nationale — Bell Canada.

Clinique d'intérêt public et de politique d'internet du Canada Samuelson-Glushko:

David Fewer, directeur intérimaire ;

Tamir Israel, stagiaire en droit.

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