House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 038 • 2nd SESSION • 39th PARLIAMENT

EVIDENCE

Tuesday, June 3, 2008

Chair

Mr. Paul Szabo

Also available on the Parliament of Canada Web Site at the following address:

http://www.parl.gc.ca

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, June 3, 2008

● (1535)

[*English*]

The Chair (Mr. Paul Szabo (Mississauga South, Lib.)): Order.

Colleagues, it's our 38th meeting of the Standing Committee on Access to Information, Privacy and Ethics.

We have two orders of business before us. One is a carry-forward item from the last meeting, as we did not get to it because of the debate we had on another motion. I'm going to suggest we get the matter on the table.

There have been some discussions, and I think what we will be doing is to have the motion moved. There will be a ruling on admissibility, and then if it's the agreement of the committee, we will suspend consideration of that motion until our next meeting so we can hear the witnesses who traveled to hear from us. That way, we can sort of start fresh on our other process of this motion.

Is that agreeable?

Mr. Hubbard, are you prepared to move your motion?

Hon. Charles Hubbard (Miramichi, Lib.): Thanks, Mr. Chair.

I read it into the minutes last time. Should I do that again?

The Chair: Yes, please.

Hon. Charles Hubbard: Circulated back on May 29—

Mr. David Tilson (Dufferin—Caledon, CPC): Point of order, Mr. Chair.

I understand the procedure you have set out. I don't, quite frankly, understand it or where you got your authority to do that.

However, if Mr. Hubbard makes his motion—and you're obviously allowing him to do that—and you rule that motion out of order, and you are challenged, we will be obliged to proceed with this today unless there is unanimous agreement that we don't proceed today. If that's the case, I trust you will be explaining to our guests why you have brought them this long distance to hear a motion they have nothing to do with.

The Chair: I hear you, and this is—

Mr. David Tilson: I think you're dead wrong in doing what you're doing, sir. I don't know where you have the authority to do what you're doing. In fact, that might be a good start: you can tell me where you got the authority to do what you're doing on this issue, particularly when initially I got a notice on Thursday, I guess it was, or maybe it was Friday, that we were going to be hearing the representatives from the Canadian Bar Association.

I then got another notice that at 5:30 today we were going to be dealing with Mr. Hubbard's motion. I then got another saying that this thing has been cancelled, and now, out of the blue today, when we arrive, we're dealing with it. It's just a continuation of a bizarre series of events of the ethics committee.

The Chair: Okay. Let me see if I can respond, just so everybody knows.

At the last meeting, as we were debating the prior motion of Mr. Martin, it appeared to me very late in the meeting that that matter was not going to be completed. I was also very well aware that we had scheduled witnesses who had to travel here, and I requested that the clerk give notice of another meeting, at the call of the chair, to continue the committee business.

As it turned out, we did in fact complete that item. I forgot to tell the clerk not to call that meeting. He followed his instructions; it was my mistake. But I don't want the members to feel there are any other things. I have already indicated to Mr. Hiebert that unless the committee agrees otherwise, our meetings are as regularly scheduled, 3:30 to 5:30 Tuesdays and Thursdays, until the committee decides otherwise.

In regard to this matter, I understand that once we get started and should we get into the situation you described, the committee can give its consent to say that in the best interests of all, and our witnesses, we should hear from them today—they're here, they've travelled here—and that there is a logical point at which we may suspend the proceedings or the debate on the matter before us, to be continued at the point where we left off, at our next meeting when we have a little bit more time to deal with it.

That is my proposal to the committee. If the committee wishes to do otherwise, I will certainly entertain any proposals. But in the meantime, I would ask Mr. Hubbard to move his motion.

● (1540)

Hon. Charles Hubbard: Mr. Chair, thank you.

I move that the Standing Committee on Access to Information, Privacy and Ethics investigate the actions of the Conservative Party of Canada during the 2006 election, in relation to which Elections Canada has refused to reimburse Conservative candidates for certain election campaign expenses, in order to determine if these actions meet the ethical standards expected of public office holders.

Mr. Chair, I'd like to thank you for ensuring that it's on our agenda today. I was disappointed on the last day that we didn't deal with it. I thought it would be a quick vote by the committee. I certainly don't want our witnesses not to be heard today.

I'm sure there's widespread support across Parliament and across the country to attempt to resolve this issue as soon possible. It's been brought up in the House on a number of occasions. I recommend that we look at it and vote on it. But if it's a matter for debate, I think we should hear from the witnesses.

The Chair: Okay.

I have spent some time in consultation on this matter and I am prepared to rule on the admissibility of the motion.

I don't have to explain to members that the matter relates to an issue in which Elections Canada has found that a political party engaged in some practice that Elections Canada claims was an attempt to circumvent the national advertising spending limits of the party and that a number of candidates were recruited to participate in those actions.

You may recall that the mandates of committees are under section 108 in the Standing Orders. Indeed, our specific mandate is laid out in Standing Order 108(3)(h), subparagraphs (i) to (vi). As with the Mulroney–Schreiber case, subparagraph 108(3)(h)(vi) states that our mandate would include "the proposing, promoting, monitoring and assessing of initiatives which relate to...ethical standards relating to public office holders". That's extremely important, and it's one of the reasons I wanted to be careful about this. As members know, public office holders are cabinet ministers, secretaries of state, and parliamentary secretaries, as well as Governor in Council appointees, of which there are some 1,200 or 1,300.

The motion before us ultimately asks us to determine whether these actions as alleged or described by Elections Canada and the actions of public office holders related to this meet the ethical standards expected of public office holders.

The question I had to wrestle with, colleagues, was that at the time of the election, there were candidates; there were no public office holders involved. However, once the election was over, the government formed, and public office holders appointed—ministers, etc., and parliamentary secretaries—one further action took place: the filing of election expenses returns by all candidates who ran in that election. Therefore, there was a formal obligation under the Canada Elections Act to file a return and to make all necessary declarations in accordance with the law.

In this matter, 67 candidates who participated were identified by Elections Canada. Of those, 17 became members of Parliament. They were elected. Of the 17, 10 are currently or at the time had been public office holders.

The four parliamentary secretaries are the Parliamentary Secretary for Canadian Heritage, the Parliamentary Secretary to the Minister of Natural Resources, the Parliamentary Secretary to the Prime Minister and for Status of Women, and the Parliamentary Secretary to the Minister of Labour.

The ministers or secretaries of state who were named by Elections Canada include the Minister of Public Safety; the Secretary of State and Chief Government Whip; the Minister of Transport; the Minister of Canadian Heritage; the former foreign affairs minister; and the Secretary of State for Agriculture.

Colleagues, this motion and our mandate can only relate to public office holders. You will find the code on the Ethics Commissioner's website. It's a 34-page document that, pursuant to the Parliament of Canada Act, must be provided by the Prime Minister.

I want to just cite a couple of quotations from this document. One is a comment from the Prime Minister:

> Our government must uphold the public trust to the highest possible standard, and this responsibility falls uniquely on all public office holders, beginning with Ministers.

● (1545)

Under the objectives and principles of the Conflict of Interest and Post-Employment Code for Public Office Holders, under "Ethical Standards", it states that:

> Public office holders shall act with honesty and uphold the highest ethical standards so that public confidence and trust in the integrity, objectivity and impartiality of government are conserved and enhanced.

As well, under the caption "Public Scrutiny", it requires that

> Public office holders have an obligation to perform their official duties and arrange their private affairs in a manner that will bear the closest public scrutiny, an obligation that is not fully discharged by simply acting within the law.

I also note that there is a compliance obligation, in addition to specific compliance, that required measures provide that "the Ethics Commissioner may impose any compliance measure, including divestment or recusal, in respect of any matter or asset", liabilities, and so on. This relates to conflict of interest. It would appear to me that conflict of interest is not what we're talking about in this matter. But it does provide a model when there is an issue such as a subsequent event.

It also says, under section 9, that within 60 days after appointment, a confidential report is required. A further report is required 120 days after appointment. The report shall include a description of all outside activities in which the public office holders were engaged during the two years prior to assuming office. It also must report all their assets and direct and contingent liabilities. I stress the contingent liabilities, because as you know, under the Canada Elections Act, when a candidate is an official candidate, the surplus or deficit is the responsibility of the candidate, not the party and not a riding association, and so on. In fact, the full disposition and responsibility are the responsibility of the candidate.

As a consequence, depending on the circumstances of an individual candidate, there may be some implications with regard to how this matter with Elections Canada is resolved by the courts and how it impacts persons. There may be some consequences to certain persons, depending on how that ruling comes out.

Finally, paragraph 15, which is related to outside activities, affirms that “Public office holders' participation in activities outside their official duties and responsibilities is often in the public interest”. It goes on to list prohibited activities and so on.

Now, having said that, colleagues, it would appear that there are issues of public interest here. There is no question that public office holders are involved in terms of filing their obligations under the Canada Elections Act and in terms of claiming expenses that relate to the matter Elections Canada has alleged and on which it has ruled, which is now being challenged in court, as you know. I won't elaborate any further.

So the question of interest, as I see it, can involve such things as whether the public office holders knew or ought to have known that their actions in regard to this matter may have been in violation of the Canada Elections Act and whether the conflict of interest code appropriately handles this kind of matter. We know that it handles conflict of interest. It certainly does not specifically deal with an alleged infringement of other acts of Canada, such as the Canada Elections Act, and whether that would require reporting disclosure and possible recusal of any parties involved in such a matter on votes or debate, pending the resolution of the matter. This is not specifically clear. An item the committee may want to consider is whether there should be amendments to the conflict of interest code.

● (1550)

We don't want to impugn any member or party in this matter. This is a very serious matter. But there is also the matter of whether or not there are any actions the public office holders should have met or may have met to meet ethical standards that are expected of them.

It may involve an assessment of whether or not due diligence was taken by them and by others who are jointly responsible for their elections return, whether or not they exercised a duty to make necessary inquiries of officials, experts, or Elections Canada, seeking rulings on matters that may have been in question, and whether or not there was an obligation or duty to report to the Ethics Commissioner and maybe even recuse themselves pending the resolution of the matter.

Also, as I indicated, under section 8 of the code there is a confidential report—

Mr. Pierre Poilievre (Nepean—Carleton, CPC): Point of order, Chair.

The Chair: Just a minute. I'm going to finish. I'm just now finishing.

Mr. Pierre Poilievre: A point of order. Recuse themselves from what, exactly?

The Chair: In the conflict of interest, recuse themselves from the matter with regard to voting or debating, participating in debate on that matter.

Mr. Pierre Poilievre: On what matter?

The Chair: In the code, under conflict of interest.

Mr. Pierre Poilievre: I didn't know there had been a vote on this matter.

The Chair: In the code under conflict of interest.

Mr. Pierre Poilievre: Has there been a vote on this matter?

The Chair: No, that is the code.

Mr. Pierre Poilievre: Okay, but there has been no vote on the matter.

The Chair: This is a bit.... Let me finish. I've got only a couple more sentences.

Mr. Pierre Poilievre: I'm curious as to what they're supposed to recuse themselves from.

The Chair: I'll take your questions, but let me finish.

Again, there is a matter for consideration of the requirements under section 8 of the code, the confidential report, where there are subsequent events that involve a public office holder that may have some bearing on the assessment of whether or not they have met the highest ethical standards, which has been asked for by the Prime Minister in this document that he is required to submit under the Parliament of Canada Act.

Accordingly, it would appear that this matter warrants consideration from an ethical perspective on standards, duties, and obligations. Accordingly, I rule that the motion is in order.

Mr. Pierre Poilievre: Chair, you didn't answer the question I posed to you.

The Chair: Okay. Mr. Poilievre, you had a question, sir?

Mr. Pierre Poilievre: You said that this had to do with a recusal from this issue, from votes related to this issue, and I didn't know there was a vote on this issue anywhere.

● (1555)

The Chair: Are you talking about the current issue in front of Elections Canada?

Mr. Pierre Poilievre: Cited in the motion, yes.

The Chair: The motion? No. The recusal I was referring to was the recusal that may be imposed on a public office holder in the event that they report a matter on which there may be a conflict of interest. The consequences would be that a member shall not participate in any debate or any votes, as you could understand, on a matter of conflict of interest.

I raise the point from the standpoint that if there is another statute of Canada under which there is an alleged infringement, there may be a reporting requirement and the commissioner may, parallel to how they handle conflicts of interest, require a recusal of that member on matters relating to the item they reported.

I give that simply as an example of some items that I found very interesting in reading this. I should also indicate—

Mr. Pierre Poilievre: Sorry, Chair, I simply have no idea what that has to do with this case at all. It seems to me that you have rambled through a lot of documents that were prepared for you that have absolutely nothing—

The Chair: No, sir.

Mr. Pierre Poilievre: —to do with the question at hand.

The Chair: Order, please.

I'm sorry. We're into debate. This is not a point of order.

Mr. Pierre Poilievre: I'm asking you a question.

The Chair: And I've made a ruling that the motion is in order. Mr. Hubbard's motion is in order.

Mr. David Tilson: Point of order.

The Chair: Now, point of order, Mr....

Mr. Russ Hiebert (South Surrey—White Rock—Cloverdale, CPC): Can you clarify? You said earlier that we would be moving to the witnesses at this point. Is that the intention?

The Chair: Well, okay.

Mr. David Tilson: I have a point of order.

An hon. member: Call the question.

The Chair: No, no. I'm sorry. The member has rights. He has asked for a point of order, and I want to hear from Mr. Tilson.

Mr. David Tilson: Mr. Chairman, I want the record to show that you made a ruling without allowing members of this committee to debate whether this motion was in order or not in order. I can assure you that members on this side would be arguing very strenuously that this motion is out of order.

You never gave us a chance to do that. You simply went willy-nilly with your ruling without giving us a chance to speak. Accordingly, Mr. Chair, I would challenge your ruling.

The Chair: The decision of the chair that the motion is in order has been challenged by Mr. Tilson. It is not debatable. I must put the question immediately.

(Ruling of the chair sustained)

The Chair: The chair is sustained.

Do we want to move to our witnesses?

An hon. member: Yes.

The Chair: And I agree.

If I may, in respect to Mr. Tilson, if I were to allow everybody to debate admissibility, we'd be going for days. I made a ruling. There is still going to be a debate on this thing.

Mr. David Tilson: Mr. Chairman, how dare you say that?

The Chair: It's exactly the way we handled it with the Mulroney-Schreiber issue. The first thing I did was rule on admissibility.

Mr. David Tilson: Sir, that is absolute nonsense. If we want to argue one way or the other, we have the right to argue. You can't just cut us off like that.

Mr. Mike Wallace (Burlington, CPC): When are we going to deal with this item?

The Chair: At the next meeting.

Mr. Mike Wallace: Can I ask you to review something before you bring it back to us at the next meeting?

I'd like to know if this motion would be in order if the court case with Elections Canada were to find in favour of the Conservative Party and it is determined that no ethical standards were violated, that we did everything legally, the party did everything legally, the individuals were legal. Would this motion not be out of order if the Elections Canada court case with the Conservative Party of Canada were resolved and the Conservative Party of Canada won that case? Would that not throw this out?

Mr. Brian Murphy (Moncton—Riverview—Dieppe, Lib.): On a point of order, Mr. Chair, I don't think you should engage in discussing the *ratio decidendi* of your decision, and what was *obiter* and what's real. This isn't *Larry King* or *The Situation Room*, where you're asked to decide the fine points of your ruling. Your ruling is your ruling.

What if the moon were made of cheese? Would you change your decision? It's silly. Don't answer it.

The Chair: Colleagues, I hear you.

Mr. Mike Wallace: You took a long time to explain why you made the decision. I'm asking you for your thought pattern on that.

The Chair: First of all, the chair is not obligated to explain to you, on your question, or to others. Let me indicate that the motion is asking us to determine whether the actions meet the ethical standards expected of public office holders, but it's not simply that issue. It's whether or not the nature of the item is properly reflected in the Standing Orders and in the code with regard to obligations. This is like an example. It's not the specifics of it, but rather an example of whether there are standards.

In any event, we have witnesses. From the Canadian Bar Association we have Mr. Gregory DelBigio, chair of the national criminal justice section; and Mr. David Fraser, treasurer, national privacy and access law section.

Welcome, gentlemen.

I apologize for the delay. It was important that we get that matter out of the way.

We know we have until 5:30 or maybe a little longer, if the members are into it, to engage you on matters of importance.

As you know, we're dealing with the Privacy Act. It's not necessarily a comprehensive review, but we're certainly focusing ourselves, as you're probably aware, on some of the so-called quick fixes that may allow us to improve the situation to some extent while consideration is being given to a more comprehensive review of the act.

I welcome you. I understand you have a brief opening statement, and I will ask you to start now.

● (1600)

Mr. Gregory DelBigio (Chair, National Criminal Justice Section, Canadian Bar Association): Mr. Chair, honourable members, the Canadian Bar Association is pleased to be here today to present our brief on the reform of the Privacy Act.

The CBA is a national association of over 37,000 lawyers, law students, notaries, and legal academics. One aspect of the CBA's mandate is improvement in law and the administration of justice. It's from that perspective that we appear before you today.

My colleague David Fraser is the treasurer of the national privacy and access to information law section of the CBA and a privacy law specialist from Halifax.

I am the chair of the national criminal justice section within CBA and a lawyer in Vancouver.

Mr. Fraser will address the issues of your review that pertain specifically to the Privacy Act. I will focus on the issue of cross-border sharing of information with foreign governments, particularly in relation to law enforcement and security.

Mr. Fraser will begin the opening remarks.

Mr. David Fraser (Treasurer, National Privacy and Access Law Section, Canadian Bar Association): Thank you for the opportunity.

We're looking at the Canadian federal Privacy Act, which when it was passed in 1982 was undoubtedly on the cutting edge of privacy legislation. But it's starting to show its age. It was built based on what are referred to as the OECD guidelines, which was a consensus of members of the Organisation for Economic Co-operation and Development with respect to changes in the way that governments collect, use, and disclose personal information.

In 1982 the federal government led the way in Canada. It was one of the first jurisdictions to implement legislation that regulated the information governments could collect, how they could use it, and to whom they could disclose it. Since then, every single province and territory in Canada has followed by implementing privacy legislation, often in combination with access-to-information legislation.

This committee has been tasked with taking a look at the Personal Information Protection and Electronic Documents Act. We've recently seen privacy laws extended to the private sector in Canada, so that now, a number of years later, we have comprehensive privacy protection from coast to coast to coast, covering both the private sector and the public sector.

Since 1982 a lot of water has passed under this bridge. We have a lot of experience in dealing with privacy legislation. We've seen it implemented in a number of different jurisdictions, and we know how it works. It's not implemented everywhere in exactly the same way, and we have had the opportunity of seeing how it works in certain implementations.

We are also living in a different world from that of 1982. Probably the paramount difference has to do with technological change. This growth in technology wasn't even foreseen in 1982. It certainly wasn't in place. We now have issues related to data matching, biometrics, genetic information, the decoding of the human genome, portable electronics, surveillance, video surveillance, GPS, and so on.

We've also seen a significant change in the environment within the public sector as information is collected, used, and disclosed. We see more joint delivery of programs by the federal and provincial governments. We also have a significantly different security environment from what we had in 1982, in the post-September 11 world.

Since 1982 we've also seen an enormous consultation among a wide range of stakeholders, primarily in the private sector. It arrived at the remarkable consensus embodied in the Canadian Standards Association's model code for the protection of personal information, which is the nucleus of PIPEDA, a piece of legislation that this committee has recently spent a lot of time looking at.

Also, there's a significant increase in concern on the part of citizens with respect to how information is collected, used, and disclosed. This is not limited to the public sector or the private sector. One cannot ignore the breaches of security related to personal information that are coming out of the private sector. But since the passage of the Privacy Act in 1982, we're also seeing significant breaches in the public sector. One hears stories of stolen servers from government departments, misdirected mail, missing tapes and backup CDs.

We're now living in the age of identity theft, and it's a significantly changed environment. In the same year that the Privacy Act became law, we also saw the Canadian Charter of Rights and Freedoms come into effect, which has changed the expectations of citizens with respect to their own personal information, their intimate details.

In our consultations with the members of the Canadian Bar Association, we have seen the growth of a consensus that in many cases guidelines—and many of the points we address are the subject of guidelines—are not enough. They may be helpful interim measures, but they're very often ignored, very easily overlooked, and don't provide sufficient accountability when it comes to the potential misuse of personal information. Legislation and therefore amendments to the Privacy Act are the only way to make sure that this happens.

● (1605)

Accountability is the touchstone of two of our recommendations, in concurrence with the Office of the Privacy Commissioner of Canada, which would be to extend Federal Court oversight with respect to privacy, and enshrine the necessity of having privacy impact assessments in legislation. Doing so ultimately leads to accountability to court and also goes hand in hand with the recommendation, which we're happy to speak to in greater detail later, with respect to the ability of the Privacy Commissioner to make public interest disclosures that are in addition to the Privacy Commissioner's obligations in reporting to Parliament on an annual basis.

Some of these measures relate directly to the significantly different criminal climate, in a sense. We're now informed that identity theft is one of the fastest growing crimes in the world, if not Canada. The Government of Canada, with its many departments and crown corporations, is the repository of significant databases with what's often referred to as "foundation information for identity theft": full names, dates of birth, social insurance numbers, and information like that, which if disclosed and misused can lead to identity theft. There are any number of government databases that contain that information.

Currently there's no statutory requirement that government safeguard that information, and there's currently no obligation that government notify affected individuals if their information is lost or disclosed. And it's not just a matter of individuals wanting to know what's happening with their information, which may in fact be their right or should be their right, but it's a matter of giving individuals the opportunity to take steps to mitigate any harm that might happen with respect to the misuse of that personal information.

An important additional maxim that's been developed with respect to best practices for the collection, use, and disclosure of personal information since 1982 is something called the "necessity test". Simply put, it's to collect only that information that is reasonably necessary, which safeguards against the natural tendency, or what appears to be a natural tendency, to collect more information than is required, which then of course requires that it be safeguarded. And if it's collected and is not necessary, it increases the likelihood that information can be misused.

We also talk briefly on the topic of data matching in our submissions, which ultimately probably does amount to, at least constructively, an additional collection of information, more than was necessary, and certainly an additional use of that personal information.

There are some other matters that are probably not as controversial but that we think are important as well.

There is a distinction between recorded and unrecorded information. There doesn't seem to be a rational reason to make that distinction. More recent privacy laws in Canada, provincial and federal, don't make that distinction. We don't think that the transient images and transient information, for example live video feeds and things like that, should necessarily be excluded from the ambit of the Privacy Act.

We do agree that five-year reviews should be necessary, and that the Privacy Commissioner should also have a public education mandate, and ultimately, in order to try to increase the efficiency of the Office of the Privacy Commissioner of Canada, discretion to refuse to investigate or to produce reports on complaints or inquiries that might be simply mischievous or vexatious or frivolous.

In the end, we do believe that ultimately the Privacy Act is due for significant reform and significant overhaul. At the Canadian Bar Association's annual meeting a couple of years ago, the national sections council did endorse a motion, which passed without dissent, calling for a complete review of the Privacy Act. But since we're at this stage, we're only given the opportunity to comment on incremental improvements. We couldn't sit idly by and do that.

With respect to our final issue, I'm going to pass it back to Greg just to touch on the cross-border information-sharing issue.

● (1610)

Mr. Gregory DelBigio: Mr. Chair, the Arar commission report illustrated the risks and complexities associated with intelligence-gathering by law enforcement agencies, the sharing of data between different agencies within Canada and abroad, and the great harm that can arise when the system fails. What is now referred to as intelligence-led policing has a potential to result in a vast amount of information being collected, not all of which is verified or even verifiable as to its accuracy.

It is our position that the existing statutory framework lacks a mechanism for effective and ongoing oversight by the Canadian government and its institutions in relation to transborder data-sharing. The existing statutory framework also does not provide an adequate mechanism for assuring compliance and accountability.

In our view, effective ongoing oversight should be mandatory, given the enormous trust that is placed in and the power that is accorded to government and its institutions in relation to law enforcement and data-sharing.

The reasons for this oversight include the following: that an individual will have no opportunity to know when a law enforcement agency has collected data about the individual; if the data has been collected, the individual will have no opportunity to learn what the data is or whether it's accurate; an individual will have no opportunity to know if data has been shared with a foreign government or institution, and if so, what foreign government or institution the data's been shared with; an individual will have no opportunity to know the uses for which the data will be used by a foreign government or institution; an individual will have no opportunity to know if the foreign government or institution will have shared the data with other governments or institutions; an individual will have no way of knowing whether the foreign government or institution that has received data will comply with any terms or arrangement under which the data was transferred by the Government of Canada; and the data may be used by a foreign government or institution in a manner or for a purpose that significantly jeopardizes the individual, the individual's family, or friends.

Further, even if an individual knows that a foreign government or institution has breached the terms of an arrangement under which the data was shared—and it is virtually impossible to know whether that is so—the individual is left with basically no recourse or remedy.

It's for that reason that the CBA has recommended what is set out on pages 18 and 19 of our brief, and in particular that:

> arrangements for disclosing personal information to a foreign government be written, formal, detailed, and public; arrangements with foreign governments or institutions that do not respect the fundamental principles of democracy, human rights, and the rule of law be very carefully considered; and a full record be made of all personal information disclosed...and the arrangement under which it is disclosed and the purposes....

In summary, it is our position that the present scheme lacks a sufficient or effective mechanism for accountability. We fully recognize—and I understand that Chief Superintendent Paulson has testified before this committee—the needs of law enforcement, the complexities of an effective law enforcement. But we urge, despite those needs and complexities, that the rule of law be maintained and upheld, and that is done through an effective mechanism of accountability.

Thank you.

The Chair: Thank you very much, gentlemen.

We have a number of members who would like to engage you in some questions.

We're going to begin with Mr. Murphy, Madame Lavallée, Mr. Martin, and Mr. Hiebert.

Mr. Brian Murphy: I want to thank you for being here today.

I'm a refugee from another committee that isn't actually sitting these days, the justice committee, but I'm happy to be here. Forgive me if I'm not as *au courant* with everything that's going on that this committee obviously has studied over the last year or so.

If I can take you to your brief, pages 9 and 10, with respect to notification of security breaches, David, I just want to get this straight. I think the gist of the third paragraph on page 9 is that there are now no legislated guidelines for notification. In the last paragraph, you say, or at least I'll say, it's too bad the commissioner did not recommend or have an explicit recommendation for a parallel statutory breach notification, mimicking a bit what PIPEDA had done.

The OPC's response, at the top of page 11, is that "It is the view of the OPC that these requirements should be incorporated into the act itself"—that is, the Treasury Board guidelines.

Do I understand that the OPC has said the Treasury Board guidelines should be incorporated into the act, but you would like to suggest that the considerations that are in PIPEDA for notification also be made part of the act, and it's unfortunate that the OPC did not specifically say that?

Is that clear?

● (1615)

Mr. David Fraser: I think there may be a little bit of confusion, because we have PIPEDA, the private sector legislation, which has been in force and was just subject to its five-year review. When it was passed, PIPEDA didn't have a breach notification requirement explicitly stated in it, but among the recommendations put towards this committee was that a balanced regime of breach notification be implemented and be amended into PIPEDA.

There is currently an Industry Canada consultation going on to determine the exact parameters of that and exactly how a balanced approach would be implemented in PIPEDA.

The Privacy Act passed in 1982 does not have any sort of breach notification. The Treasury Board, obviously to their credit, has implemented policies, procedures, and guidelines to deal with security of information, including breaches related to that information.

The Canadian Bar Association is advocating on both sides—within PIPEDA, the private sector legislation, and in the Privacy Act, the public sector legislation—that there be breach notification guidelines. We have not taken a specific position on the specifics of them in terms of what information would have to be disclosed in order for the individual to be notified, because it is a matter of balance. You don't want people to be bombarded by notifications about trivial breaches, but you do want to make sure that individuals whose information is compromised in a way that could actually have a significant impact on them are notified. So we're advocating in both pieces of legislation that there should be balanced notification.

Mr. Brian Murphy: Since you brought it up, what's a trivial breach?

I know there are a couple of highly publicized and sometimes inadvertent breaches with respect to health records. I can think of my own province of New Brunswick; it happened. Or passport information. I think we are on common ground that those are not trivial.

Mr. David Fraser: We don't specifically say within the brief, so I'm kind of moving into my own views on this, but yes, I would say those are not trivial.

Mr. Brian Murphy: Let's not get into what trivial is, but on those we can agree that there should be some legislative requirement to notify someone that their privacy has been breached. We're on common ground here with that.

Mr. David Fraser: Sure, and it does—

Mr. Brian Murphy: I'm trying to figure out what is the higher standard. Is it the Treasury Board guidelines as they exist under the Privacy Act? They're not law, but they're guidelines if they're followed. They're moral law, if you like. Or is it the discussion that's surrounding what there will be for PIPEDA?

Mr. David Fraser: It's our view that the government should be controlled with respect to the security safeguards and notification rules to standards at least as strong as will be in the private sector.

It's an important maxim—at least in the more modern principles of personal information protection—that information needs to be treated according to its sensitivity, and some information is more sensitive than other information. The information on your tax return or my tax return would be considered to be more sensitive than the information that's on my annual pass to a national park. So one needs to take into account the sensitivity of the information in order to determine what measures and safeguards need to be implemented, and at the same time take that information into account as to whether one needs to notify.

● (1620)

Mr. Brian Murphy: I can think of one set of hearings we had in which the tax information of a particular witness was very much at issue, and we were unable to discuss the sensitivity of it in any detail—but that may come another day.

Finally—this is more philosophical, and I can see it going both ways and want your brief opinion on it—for government to work, there has to be some disclosure of personal information. I can think of no instance where, in the private sector, they have to have information. If you want the privilege of getting a loan, you have to give information; that's fine, but I can think of no forced reason for it. Government is a little different.

On the other hand, our government is in a fiduciary relationship with us, so the care must be higher. Given that the government has to have some information but the relationship is much more a fiduciary one, I wonder whether the balance is that it should be the same standard as for the private sector, as is contemplated in PIPEDA, or do you think it should be held to a higher standard of notification?

Mr. David Fraser: On the philosophy or the difference, you've really hit the nail on the head with respect to the principal differences between the private sector legislation, where it concerns a consensual relationship, and the public sector legislation. When you're dealing with a bank or dealing with your local video store, you have the opportunity to go elsewhere, so consent is really the bedrock of it. It's about informed consent, and that links to principle two and principle three within PIPEDA.

A citizen does not have a voluntary relationship with the government. Perhaps when it comes to certain services and whether the individual chooses to take advantage of those particular services, there is a bit of the voluntary, but a citizen's relationship with Revenue Canada, the employment insurance commission, or other departments is not voluntary whatsoever. The individual has an obligation. One can't necessarily ask for consent.

Mr. Brian Murphy: Just in hindsight, do you think there should be different centres within government?

The Chair: I'm sorry, Mr. Murphy. I really have to manage the clock here to be fair to all.

Madame Lavallée, *allez, s'il vous plaît.*

[*Translation*]

Mrs. Carole Lavallée (Saint-Bruno—Saint-Hubert, BQ): Thank you very much, Mr. Chairman.

I want to come back to the recommendations as a whole. If I understand correctly, you took the commissioner's recommendations and commented on them. If I understand correctly, you agree with the ten recommendations, but you have added another one, which deals with notification.

Have you added any others?

[*English*]

Mr. David Fraser: I believe notification was one of the ones the commissioner recommended. We added the general duty to protect personal information and the issue respecting data matching, if my recollection is correct.

[*Translation*]

Mrs. Carole Lavallée: You may be right, but I can't find the recommendation dealing with notification.

[*English*]

Mr. David Fraser: My apology; I believe it is included in the necessity one.

One moment.

[*Translation*]

Mrs. Carole Lavallée: I for one have not seen it. It was not included in any of the 10 recommendations.

[*English*]

Mr. David Fraser: I'm sorry; my apologies.

The first two, the duty to protect and the data matching, were considered separately, and they were considered to be at least connected to the reporting by the federal Privacy Commissioner.

Within the discussion we had at the Canadian Bar Association, because we weren't looking at a complete overhaul of the Privacy Act, we were looking to consider the issues we thought were the most significant and thought that if there were a limited amount of attention that could be given to the Privacy Act, we should focus on those. Breach notification is related to other issues that the commissioner brought up, but it's also seen as something that needs to be considered, and considered consistently as between the private sector and the public sector.

[*Translation*]

Mrs. Carole Lavallée: So you would put that in as recommendation number 11.

● (1625)

[*English*]

Mr. David Fraser: I don't have them numbered separately.

[*Translation*]

Mrs. Carole Lavallée: The commissioner numbered them.

So you are making that recommendation in addition to the ones already presented. Some witnesses have made other recommendations. I would like your opinion on, among other things, the commissioner's quasi-judicial power to make orders.

The commissioner said that she did not need that power in order to do her work. But some witnesses have indicated that no one would take a commissioner seriously that did not have the power to make recommendations or act as an ombudsman.

[*English*]

Mr. David Fraser: Without having turned our minds explicitly to the narrow question of whether the commissioner in this context should have order-making powers in the Privacy Act rather than PIPEDA, the consensus seems to be that in order for there to be proper accountability within the legislation, there needs to be a mechanism to make sure there's accountability for the statutory requirements set out within the Privacy Act to an external body, be it the court or the Privacy Commissioner.

The consensus we reached was that the Federal Court of Canada should have the ability, on the motion of an individual citizen or the Privacy Commissioner of Canada, to require a government department, crown corporation, or another public institution affected by the Privacy Act, to follow all of the requirements of the Privacy Act, not just the ones related to the access to personal information.

[*Translation*]

Mrs. Carole Lavallée: I am sorry, but I do not understand. You say that you have not looked at whether the commissioner herself should have order-making power. You also say that a body outside the commissioner's office should be able to require individuals, officials or federal institutions to comply with the act.

[*English*]

Mr. David Fraser: I just want to make sure I fully understand your question.

[*Translation*]

Mrs. Carole Lavallée: We are having a bit of difficulty.

[*English*]

Mr. David Fraser: There are a number of different models. There's the one that would give the commissioner the power to compel a public body to follow the requirements of the law. Currently it's not the court nor the Privacy Commissioner; it's simply a requirement that every citizen and every employee of the crown follow the law, but there's no particular accountability.

Without completely revisiting the role of the Privacy Commissioner of Canada—which is currently in the model of being an ombudsperson—the best way to do it, as an interim measure at least, is to give the court that power and leave the Privacy Commissioner of Canada within the ombudsperson sort of model it is.

On whether we think that giving the Privacy Commissioner order-making powers would significantly change the role of that office and the person in it, that debate should probably take place in a wider debate about more comprehensive reform of the legislation.

[*Translation*]

Mrs. Carole Lavallée: Thank you.

You talked earlier about notification regarding situations where there were potential violations or disclosure of personal information. If I remember correctly, the committee's recommendation was that businesses would be required to notify the commissioner in those types of situation under the Personal Information Protection and Electronic Documents Act. The commissioner would decide whether the people concerned would be notified. It might be good to add that possibility, after all.

Thank you.

[*English*]

The Chair: Mr. Martin, please.

Mr. Pat Martin (Winnipeg Centre, NDP): Thank you, Mr. Chair.

Thank you to both of the witnesses. It's been very interesting.

I don't know if I fully understand Brian's comments that the Privacy Act should have the same duty of notification provisions as PIPEDA. One of the big flaws of PIPEDA is that it doesn't have the duty of notification, and when our committee studied it we recommended unanimously to the government that it should have duty of notification. But when the government reacted to our report, tabled in Parliament, they said clearly the government is not interested in putting duty of notification into PIPEDA. So I don't think we're any closer to having that duty put into statute at all, which is really worrisome to me, because a lot of Canadians would be horrified to know or would want to know if their personal information was compromised in the private sector or the public sector.

The PIPEDA report was just tabled in Parliament today by the Privacy Commissioner. You might want to get a copy of that. It talks about the TJX case, where personal information and 94 million debit card and credit card numbers were compromised in that one violation alone. There were 94 million—they weren't all Canadians—people from around the world, I guess. This is worrisome to me, and I think the Privacy Act should have a rigid duty of notification.

The cross-border sharing of information is of great concern to us. I want to thank you for bringing your input into this, and specifically citing the Maher Arar case as a graphic illustration of what can go wrong and has gone wrong.

Is there anything more you can tell us about the Canadian Bar Association's views on this? Or would you like to speak a little more on the subject of how we might prevent another Maher Arar incident?

● (1630)

Mr. Gregory DelBigio: Certainly the CBA has taken positions in relation to this issue really since the anti-terrorism legislation was tabled. And we have appeared before different committees and we have expressed concern with respect to the need to have appropriate checks and balances in place.

We recognize it is very easy to speak in generalities such as that, to say that it is important to have the checks and balances. And it's equally easy to make remarks such as that it's important that there be effective law enforcement. What that actually looks like in terms of the drafting of a statute, for example, is very, very difficult. But one must start from first principles of agreement to ask, is it agreed that there should be a mechanism of accountability?

We have taken the position that it should be an independent body. So our position is that the RCMP, for example, should not be responsible for their own oversight on these types of issues. And because it is an independent body that is disinterested in an ongoing issue, that can perhaps most effectively ensure compliance or an accurate audit of what is actually going on.

What can be learned? Well, hopefully the specific incident of Mr. Arar...all of Canada must desperately hope that this will not be repeated.

Is there a mechanism in place to ensure that it will not be repeated? I'm not sure, because what is going on is there continues to be, as I understand the allowances of law, a vast amount of information gathering and information sharing between agencies within Canada and abroad. And until one knows exactly how much information is being gathered and what information is being gathered and why it is being gathered and who it's being shared with and whether that sharing mechanism has appropriate checks and balances, it's really impossible to know whether or not some of the mistakes of the past will be repeated.

Mr. Pat Martin: That's very well put.

With what little time we have left, you've led me to another thought. This committee wrestled with section 7. Paragraph 7.1(e), I believe, of the national security legislation essentially gives the government the right to deputize others to intrude into a person's private information. One of the examples used was that a government couldn't open up a worker's locker without a warrant, but they could have the employer do it and pass that information along to them, if they have a third party do an end run around your rights to privacy through the national security legislation.

Do you know what section I'm getting at here?

● (1635)

Mr. David Fraser: Are you referring to paragraph 7(3)(c.1) of PIPEDA?

Mr. Pat Martin: Yes, that's it exactly. It's somewhere in there. That's right. It was in the context of the long review of PIPEDA that we did. I guess the law association has made representation, perhaps, on that clause in the past, and you're aware of the point I'm raising. Would you care to expand on that?

Mr. David Fraser: That particular provision is in PIPEDA, and much of the debate relates to some uncertainty regarding its interpretation. But ultimately, it allows the disclosure of personal information, without consent of the individual, to a law enforcement body or a national security body that has requested it, has identified its lawful authority to have it, and says that it's for the purposes of law enforcement or for enforcing a law.

Currently there's virtually no analogous restriction in the Privacy Act that we have before us. For example, the RCMP and Revenue Canada are both institutions of Her Majesty or the crown, which are indivisible; they're just organized in different sorts of ways. So information shared within one department or shared between two departments does not amount to a disclosure in the same way that under the private sector legislation it would be.

Under the current legislation, there is no necessity test or necessity requirement for that information. There's not even an obligation on the part of the law enforcement body to identify that it has the lawful authority to have that information, or even that it relates to a particular purpose.

It is my understanding that there are memoranda of understanding between government departments with respect to the sharing of that information, but those memoranda of understanding don't go through the checks and balances my colleague just referred to. They don't receive the same sort of scrutiny. The Privacy Act, as it's currently drafted, doesn't stand in the way of any of those sorts of practices.

Mr. Pat Martin: That's interesting.

The Chair: Mr. Hiebert, please. You're up again.

Mr. Russ Hiebert: Thank you, Mr. Chair.

A number of questions come to mind.

One thing that the Privacy Commissioner mentioned was that a lot of complaints—in fact, the single largest source of complaints—her office receives are from inmates in Canadian correctional services, and she felt that many of these were frivolous or vexatious.

While I'm sure there are certain complaints from inmates that are legitimate, it does seem strange that so many of them are coming from that area, a much higher number than from any other area.

Mr. DelBigio, since you have some background as a defence attorney, can you explain to the committee why there are so many complaints coming from this area? What are they used for? Why would this be the case?

Mr. Gregory DelBigio: I can't comment either through my day job as a defence lawyer or in my capacity as a CBA member. I did read somewhere that this had been an issue before, that there had been evidence to this effect before this committee. And I'm sorry that I really couldn't give you an answer to the question beyond mere speculation.

Mr. Russ Hiebert: Mr. Fraser, do you have any idea why this is happening?

Mr. David Fraser: I don't know the specifics of it. I certainly am aware that the Privacy Commissioner has said that.

The Correctional Services of Canada is an institution under the Privacy Act. Individuals would have a right of access to their own information. I certainly have seen instances in which access to information provisions, under privacy legislation or under access legislation, public and private sector, are used in order to get information either as an antecedent to litigation or as a substitute for it, or just as part and parcel of somebody wanting to find out what somebody else has on them. They may simply be an instrument of individuals to find out what information there is about them that is being held by the institution.

Mr. Russ Hiebert: So I guess either of you would be in a position to help us figure out how to address this concern.

Mr. Gregory DelBigio: I should add that certainly it is my understanding that the information the corrections service might hold in relation to an individual might be relevant to issues such as classification within the prisons, or perhaps even parole eligibility. So to the extent that the personal information is going to relate to those issues, it is going to be of obvious interest to an individual. And that interest is going to be engaged if a person believes he or she should be held in a prison of lower classification, a lower-security institution, or if the person is being denied parole and the person contests that.

● (1640)

Mr. Russ Hiebert: On page 11, under section F, which is dealing with recommendation number 6, you suggest that the Privacy Act should be amended to authorize the commissioner not to prepare a report in specified circumstances. What kinds of circumstances are you contemplating?

Mr. David Fraser: What it comes down to, ultimately, is that the Privacy Commissioner has scarce resources, scarce staffing, just as every other government department. Also, as of necessity, every individual has a right to make a request for access to their own information, about the existence of their own information, and otherwise. There's a very low barrier to entry, and that's important, for individuals to exercise their rights of access under the Privacy Act.

The concern is, and it has been at least a position taken by the Privacy Commissioner, that there are inquiries or complaints generated that might amount to being frivolous or vexatious, or might have been initiated for collateral purposes, so in order just to be an irritant rather than actually exercising what amounts to a legitimate right.

We are suggesting that if there is a reasonable basis to believe that this is the case, no purpose would be in fact served by proceeding further with a full investigation, with producing a report, to provide a mechanism to short-circuit that. While not addressed within our report, if the commission were to make a decision like that, and the individual was sufficiently aggrieved and believed they did have a legitimate case, they would have the opportunity, under other legislation, to seek judicial review of that decision, to have a judge take a look at it.

So it would include, one would hope, the protections to make sure that only in fact those cases that are frivolous, vexatious, or malicious are short-circuited at that particular point.

Mr. Russ Hiebert: Right. You're saying the commissioner would have the opportunity to say this particular complaint is frivolous or vexatious and it's not in the public interest, but at the same time, that individual who made the complaint could then appeal that decision to the Federal Court. Is that not your recommendation number 2?

Mr. David Fraser: Recommendation number 2, with respect to a Federal Court oversight, relates specifically, or at least within the four corners of our court, with an ability to order a government department to follow the requirements of the Privacy Act. So it doesn't relate specifically to the enforcement mechanism or to requiring the Privacy Commissioner to do or to not do things.

Mr. Russ Hiebert: So an individual would not have the opportunity to appeal to the Federal Court if they disagreed with the Privacy Commissioner.

Mr. David Fraser: They would have a slightly different procedure under a different statute, the Federal Courts Act, which allows you to seek judicial review of any decision. So it wouldn't amount to an appeal under the Privacy Act.

Mr. Russ Hiebert: The chair is telling me that my time is limited, and I have an additional question. So I'll leave that discussion aside for a moment.

Dealing with recommendation 9, on page 12, section H, the five-year statutory review, you suggest, without any explanation, that this committee review this legislation every five years. Now, you may or may not be aware, but we haven't reviewed this legislation in 25 years, and it's not likely that there would be a desire to do it as often as you suggest.

I'm wondering if you could help us understand why you think the time and expense would be necessary to review it every five years, keeping in mind that we understand that with PIPEDA things change frequently in the marketplace, and there's certainly a need to review that every five years. But with respect to this legislation and the less frequent change in how the public interacts with the government, what would be the value in reviewing it so often? Would it not suffice to do it less frequently?

Mr. David Fraser: In my opening remarks I did list a number of the factors that contribute to our belief that even though the fundamental relationship between the citizen and their government is relatively static, the information management practices, the complexity of the information that's collected, the consequences of that are changing just as rapidly in the government sphere as in the private sector.

While we're not purporting to say that a full comprehensive review needs to be done every five years, at the minimum there needs to be a bit of a reality check to make sure that this important piece of legislation that's been identified by the Supreme Court of Canada as being quasi-constitutional actually does keep up with the requirements of modern society. And it's our view that it hasn't. The world has changed significantly. The government information practices have changed very significantly since 1982, and it's very difficult to say what the next five years, ten years, fifteen years are going to look like.

● (1645)

Mr. Russ Hiebert: This is why I'm so glad we're taking the time to review this at this present time. And I hope we're not derailed.

The Chair: Mr. Hubbard, please.

Hon. Charles Hubbard: Thank you.

First of all, I'm very pleased with your submission. It really goes number for number with the various recommendations the Privacy Commissioner has made.

As practising lawyers, have you had any direct interventions on behalf of your own clients with the Privacy Commissioner or her office?

Mr. David Fraser: With respect to the particular matters enumerated within this?

Hon. Charles Hubbard: If you go back to 1982, have you had clients that said they were having trouble under the Privacy Act and you dealt with the privacy commission on their behalf?

Mr. David Fraser: Taking off my CBA hat and putting on my private practice hat, one of the differences between a piece of legislation like the Privacy Act and other pieces of legislation is that it's essentially designed to be user friendly. For example, the primary right that's given to citizens under this piece of legislation is the right of access to their own information. It sets out a scheme through which they can, without the assistance of lawyers, fill out forms and ask for their own information.

But to get directly to your question, people have asked why they are collecting this information, and my response has had to be “Because they can”. They ask what they can do about it, and I answer “Not much”.

Hon. Charles Hubbard: One group that probably avails themselves more of this act than others would be the 300,000 people who work for the public service. Those who apply for jobs within the public service can apply under the Privacy Act to find out why they weren't promoted, why they didn't get certain jobs, why they weren't hired. From that point of view, I think that every manager has to be very much concerned with what he or she does with data in terms of working with people.

Do public servants have a fair showing in terms of privacy legislation, going back to 1982? You see soldiers who say "I didn't get my sergeant's rank", or "I didn't get my promotion to major", or "Someone has written a bad report on me, and I would like to get a copy of that report".

I do know that many federal institutions are reluctant to provide the complete details on particular individuals when they request that information. With the present act and the changes we're talking about here, will it in any way enhance the ability, or will it be a further problem to managers within the public service? If a job is open and ten people apply, only one person gets it and there are six people who are dissatisfied, how big an operation are we involved with in terms of the privacy legislation?

Mr. David Fraser: It's very interesting that you highlight the access to one's own information, which is likely the way the Privacy Act is used most often. It most immediately has an impact on the lives of individuals who are employees of the government, but also individuals who want to know the basis for decisions that are made about them.

A central maxim of privacy legislation is access to one's own information. It's interesting that these recommendations don't suggest a significant overhaul of the access to one's own information. They relate to the collection, use, and disclosure of personal information by government institutions and by public bodies.

To ultimately answer your question, I hope, I don't think the changes we have suggested are going to dramatically change that and either lead to a stampede of individuals asking for their own information or somehow restrict or hamper supervisors in that particular capacity.

The one that comes to mind, which would most particularly have impact on that, would be the requirement that one collect only information that's reasonably necessary. I could see it happening, for example, in the hypothetical situation you put forward of somebody doing an evaluation of potential candidates for employment or promotion. If the supervisor has used information that really isn't necessary or relevant to that decision, they would have crossed the boundary within the privacy legislation. They would have gone too far in collecting information that likely would be irrelevant, or too intimate, or what have you.

● (1650)

Hon. Charles Hubbard: Thank you.

Paul, am I done?

The Chair: Yes, you are, sir. Right on time.

Mr. Wallace, please.

Mr. Mike Wallace: Thank you, Mr. Chair.

Thank you, gentlemen, for coming.

Mr. Fraser, in your private practice, what kind of law do you practise?

Mr. David Fraser: I practise privacy law and information technology and IP law.

Mr. Mike Wallace: Okay, thank you.

If I heard you correctly, if you had your choice from an organizational point of view and you were giving us advice, instead of what the committee has sort of framed itself around thus far, the organization that you represent would have liked us to do a much more thorough review of the act, clause by clause or whatever you want to call it, since it has never really been reviewed to that extent since its inception. Is that correct?

Mr. David Fraser: Yes.

Mr. Mike Wallace: Okay, I appreciate that.

I have a couple of questions on your recommendations here. I'm going to give you a real example. I intended to ask the Privacy Commissioner about this when she came back, because I didn't know what the rules actually were.

The first recommendation I have highlighted is on page 4, where you talk about "federal institutions to link personal records in computer systems only if the linkage would not reasonably be expected to harm individuals whose information is being disclosed". Right now, if I understand you correctly, one department can tell another department that if they have information on me, they can give it to another department and there's nothing really stopping them from doing so. Is that correct?

Mr. David Fraser: Within the current legislative scheme, yes.

Mr. Mike Wallace: Is there an exception of some sort?

Mr. David Fraser: Well, there are guidelines with respect to that.

Mr. Mike Wallace: So maybe you can help me with this. In round numbers, we have 60,000 people who are here illegally. We know where some 20,000 of them are; 40,000 we don't know. Many of them have SIN numbers and are paying taxes. They've been in my office in Burlington.

In the view of your organization, does the Government of Canada have the right to have the immigration department know where those people...? When people put their taxes in, their address is on their tax return, so CRA has it. Should the government be able to use that information from CRA to assist the officials in immigration and border security to be able to find those people, or would you consider that harming individuals if that information were disclosed? I'd like your opinion.

Mr. David Fraser: I'm absolutely confident that particular scenario didn't go before the committee that developed these recommendations. What we recommended was a framework so that the government departments in question, subject to oversight or consultation with the Privacy Commissioner, could make that particular decision.

Mr. Mike Wallace: I'll ask the Privacy Commissioner that specific question when we see her again.

I hate to put you on the spot, but I'm trying to find out where the limits are in terms of whether there are limits or whether people are expecting limits. In my view, as the Government of Canada, if people are here and have been ordered to leave, they're here illegally, and we should work with whatever resources we have to fulfill those requirements for them to leave. For people who have come here legitimately, or are trying to get here, we should spend our time and resources making sure that happens.

My next question comes from part of the recommendations of the commissioner. Hers are slightly different, unless I'm reading it wrong, and that's why I'm asking you. On page 7, you ask about the PIAs, the development of any new programs and policies that involve the collection and use of data, that there should be an amendment to the Privacy Act requiring the bodies to do it. I think it's what she's recommending; I simply want to be sure. At present, there are policies around departments requiring them to do it. Do you believe it should be in the legislation as a legal requirement?

● (1655)

Mr. David Fraser: Yes.

Mr. Mike Wallace: Are you aware of any situations or anything where the policy piece that Treasury Board has put out to all departments is not working? Do you know if it's not working?

Mr. David Fraser: The privacy impact assessment framework that has been put out by Treasury Board I think reflects a lot of thought that went into it, and I think there is no information to suggest that it's not being properly implemented. I think what this recommendation reflects is that it's a very important practice; it's a very important tool to understand the context and the consequences of any change in government programs, be it data matching, be it extending a program or otherwise, and to make it mandatory, much more so than simply a guideline. There's no accountability for not following a guideline, other than potential employment consequences.

So the issue, ultimately—particularly combined with the ability for the courts to enforce it and to order it—is to make sure that these things do take place.

The Chair: Thank you.

I have Mr. Nadeau, followed by Mr. Van Kesteren and Mr. Martin.

[*Translation*]

Mr. Richard Nadeau (Gatineau, BQ): Thank you, Mr. Chairman.

Good afternoon, gentlemen.

The commissioner's sixth recommendation deals with the power to reject or drop a case. What is your opinion on that? Do you think that such a power should be granted?

[*English*]

Mr. David Fraser: We have recommended, in concurrence with the Office of the Privacy Commissioner of Canada, that in the event it is reasonably considered that it would not ultimately be advantageous to take a question or inquiry to a full investigation and ultimately to a report, the Privacy Commissioner have the ability, once she has made that determination, to end the process there.

I don't expect it would be used very often; it would only be in those explicit cases. But it would ensure that the attention of the investigators and analysts was focused appropriately on the right cases, rather than perhaps following a formalistic process in those cases where it's not going to result in any real advantage for the individual.

[*Translation*]

Mr. Richard Nadeau: Witnesses who came before the committee did have some reservations. Is this something that happens often at this point? Should certain mechanisms be changed or improved to allow for that, while ensuring that those who file complaints do not feel that their rights have been violated?

[*English*]

Mr. David Fraser: There are similar provisions. In my own experience and understanding, courts are asked from time to time to consider somebody as a vexatious litigant, so they are not able to file complaints, lawsuits, or other process with the court, except with the permission of the chief justice. They are simply seen to have been abusive to the court process. It's that same sort of mechanism.

I do not have—and I do not believe our committee considered—actual statistics on what the commissioner considered to be the number of inquiries or questions that were put into that category, but I expect it would be a reasonably small number.

[*Translation*]

Mr. Richard Nadeau: I would like to move on to something else.

Regarding coordination with foreign countries seeking information, we met with representatives from CSIS and the RCMP. We could not explore all aspects of the issue because our time was limited. There is something that bothers me a bit. CSIS and the RCMP are two separate silos. Either one can deal with a request from within Canada or a foreign department without the other knowing it.

Do you think that some things would need to be looked at more closely? I do not know if this is the correct term, but people talk about data matching. Would it be important to make sure that the left hand knows what the right hand is doing with respect to a given case?

● (1700)

[*English*]

Mr. Gregory DelBigio: I hesitate, because I certainly don't want to speak on behalf of either agency. They will be pleased. But the mandates are separate, so it is entirely conceivable to me that there will be instances in which each is working with a foreign country advancing their individual mandates in a way that is not coordinated with one another.

As to what extent there should be better information-sharing or coordination between them, I think representatives of either of those agencies might best address that type of question.

[*Translation*]

Mr. Richard Nadeau: I would have thought that you would have an opinion on this issue since they told us that independence is what it is for each of the entities. The whole issue of national security... Without being an expert in this field, it seems to me that it is unusual that two important institutions do not know that they are each dealing with the same country on a given file.

We would like to improve this act. According to your recommendations, which changes are the most urgent and would result in improvement, given that we may not be able to do everything all at once? Are there any aspects that require a change like the one we had yesterday, compared to others that may be implemented over time? Would it be acceptable to prioritize some aspects of your recommendations?

[*English*]

Mr. David Fraser: You'll notice in our submission that we didn't rank them or say that this one was more important than the other. Without having asked the question to the group that put together the report and consulted with the members of the subsections involved in its production, I would hesitate to say what would be the highest priorities.

We have identified and concur with the Privacy Commissioner that at least the ten recommendations she put forward are important and should be addressed now. We have identified, in particular, two additional ones that bear close thinking. It would be a shame to open up the Privacy Act for review without having at least made an attempt to implement these twelve recommendations to the extent possible.

I hesitate to make a guess or purport to speak on behalf of my colleagues.

The Chair: Mr. Van Kesteren.

Mr. Dave Van Kesteren (Chatham-Kent—Essex, CPC): Thank you, Chair.

Thank you both for coming. We really appreciate your being here. I think you bring a whole lot of knowledge to the table.

Just very quickly, your recommendation on page 4 talks about harm to individuals, but who would deem it to be harmful? Who would have the responsibility to deem what is harmful? Is that something the courts would do?

Mr. David Fraser: What we are looking at is a situation with privacy legislation where you're trying to anticipate and put in place rules that are going to be applied—or hopefully are going to be applied—in a huge diversity of circumstances. So almost by necessity, there has to be language that talks about principles rather than rules. It's not necessarily a yes or no, but of looking at the totality of the circumstance and asking, is this reasonable or is this not? Ultimately we're trying to come up with an objective standard, which would likely be would a reasonable person consider the result of this project, or the possible likely result of this project, to be harmful. Ultimately, the courts do step in and take that role.

● (1705)

Mr. Dave Van Kesteren: Page 6: I'm a little bit worried about that recommendation. There seems to be a problem with inmates, and I'm a little afraid that this particular recommendation would worsen that problem. That's just a personal observation.

I think the recommendation on page 11 is good. I think that's necessary.

Page 12: when we get to the final list of recommendations, I begin take issue. I really don't care if foreign governments have my information. Mr. Fraser, you said somebody would ask, “Why are they collecting this information?” and the answer would be, “Because they can”. The question then was, “How can I make them stop?” Why?

What are worried about if we don't have anything to hide? I'll tell you why I'm leaning towards this. I had an interesting chat with a criminologist. I know Mr. Martin would quickly bring out Mr. Arar's case, but that was a case where we had just had 9/11, and we made a bad judgment call. I'm wondering, don't we correct that?

Getting back to the criminologist, the biggest challenge to law enforcers today are criminal elements. It's the criminal elements who use these. I'm not being judgmental, but I want a balance here. I would think if you were drafting up something you'd probably be representing mostly criminal elements when you talk about people who are concerned about privacy. If you were a criminal, you'd want to have laws that would enable you to win your case. Do you understand what I'm saying?

I'm not being judgmental. I'm not saying you're being cynical. I'm just wondering if that's not what we're doing, if we're not protecting the criminal even further. It's so difficult now for law enforcement agencies. It's so difficult for governments to handle terrorist groups. Why would we want to make it that much more difficult?

Mr. David Fraser: Your question had a number of elements. I would like to break them down.

With respect to things that happened after 9/11 and our correcting them as we move on, we believe that this is part of this correction. I'll try to address the balance of your question.

Ultimately, this is about trying to find a balance. We're in a different world, security-wise, than we were a little while ago. We're in a different world, technology-wise, than we were a while ago. This affects both the common way that individuals communicate and the way that people who want to evade being intercepted communicate. And this in turn affects the investigative tools that law enforcement have at their disposal.

We're not looking at dramatically altering the balance. It's not up to the Privacy Act to determine the proper balance with respect to law enforcement and private laws. This comes under the Charter. We're looking at putting in place a framework that deals with the reality that we're living in an age of identity theft, where the more information that an organization has about somebody, the more safeguards they have to implement to prevent the greater harm of accidental disclosure of that information. So there are protections with respect to that.

The Chair: Good questions.

Mr. Martin.

● (1710)

Mr. Pat Martin: I don't have much more to add, other than that I'm enjoying reading some of the background that you've given us regarding data matching.

The one example I'd like to run by you is similar to what Mr. Wallace cited as an example. We found this one worrisome. The federal government knew that 300,000 senior citizens were eligible for the guaranteed income supplement but had never applied for it. They knew this by virtue of their income tax returns.

We asked the officials, if they knew these people were eligible, and they knew they were in need, because they had to be really low income to be eligible, why they didn't just tell them that they qualified for another $12,000 a year. Their answer was that it would be a violation of the right to privacy to use income information for any purpose other than assessing taxes on their income.

Does that jibe, does it seem plausible? Given what you know about the Privacy Act, was the government acting properly in not using their income tax information for any purpose other than income tax?

Mr. David Fraser: I'm not sure I can comment on that specific one. I would expect it has to do with the particular requirements that are not in the Privacy Act but in the Income Tax Act that are specific about the confidentiality of tax return information, which recognizes the high measure of sensitivity and the fact, for example—

Mr. Pat Martin: But Brian Mulroney says it's safer.

Mr. David Fraser: Because it's a self-reporting system, the legislation allows you to even report criminal sources of income because the interest is seen as being in collecting taxes rather than doing other things.

Mr. Pat Martin: Is that right? I know that's not what we're here to talk about, but you mean under the Income Tax Act, if you did report income from illegal sources, Revenue Canada couldn't use that against you to turn you in, as it were? They wouldn't know, though.

Mr. Gregory DelBigio: There are mechanisms for sharing that information.

Mr. Pat Martin: There are mechanisms, of course, disclosing... money laundering and stuff like that.

As another example, the border guards turned in a carload of people who were on EI, employment insurance. When these people were coming back into Canada, having gone for a day trip to the States, the border guards somehow learned they were on EI and turned them in. You're not allowed to travel out of the country while you're supposed to be actively looking for work in this country. Wouldn't that be a violation of these people's right to privacy?

Mr. David Fraser: Under the Privacy Act as it's currently structured, it's my understanding that it is not. I believe there is case law whereby if you return to Canada on an aircraft, information from that form you fill out is matched against information in the EI database to determine whether or not you were vacationing in Florida. That was the exact case. So data matching does take place.

Mr. Pat Martin: So that's not contravening your right to privacy as a Canadian citizen, if I choose to break the law.... I don't think I'm going to go any further down this.... I'm on dangerous territory, I agree.

Is that an example that brings us back to where I started—that's what you call data matching, computer matching?

Mr. David Fraser: My recollection is the courts found that to be lawful. What we're talking about is not just those particular examples, because data matching can be used for any number of purposes, both in the law enforcement context or immigration enforcement, and in other contexts as well.

We're saying there needs to be some significant thought given to it, because it might simply be a matter of convenience of wanting to match this information, because information is extremely useful. Revenue Canada, the Government of Canada, runs on information, there's no doubt about that.

But when information becomes centralized, it becomes more potent in the sense that it is potentially more dangerous to the privacy interests of individuals. It's potentially more dangerous if that information is leaked. One would probably recall a number of years ago Human Resources Development Canada launched LLFF database that took employment insurance information and income tax information, information from a number of sources. So it had individuals' histories, employment histories, going back from beginning to end, all in one database. It was seen as being lawful, but politically problematic to such an extent that it had to be dismantled because there were very strong feelings that it was not appropriate.

So what we're talking about is not saying that this is okay and that's not; it's making sure there's a framework in place to make sure those important questions are asked at the time.

● (1715)

Mr. Pat Martin: What specifically was wrong with the RCMP database that the Privacy Commissioner felt compelled to make a special report to Parliament that they had compiled this massive database?

Mr. David Fraser: I'm not sure I know enough of the specifics to answer that.

Mr. Pat Martin: I'm sure it's available to us.

The Vice-Chair (Mr. David Tilson): I think your time has expired. If you wish to speak again, you can, but we'll go now to Mr. Murphy.

Mr. Brian Murphy: Thank you, Mr. Vice-Chair.

I want to get back to this standard review of public-private. I may be fixated on this health issue, but records that were gathered by a public agency were sent to a private company for a process, and I suspect this might happen more and more as governments try to find ways to deliver services more economically.

I'm not starting a diatribe totally against the whole public-private partnership thing, but there has to be an understanding of whether this was a public function or a private function. I live in the world of examples, unfortunately, but when you have a public agency that gathers the information and gives it to a private company.... Back to my question a while ago, do you think there should be any different standard, and whose breach is it?

Mr. David Fraser: That exact circumstance is not explicitly addressed in the Privacy Act. In PIPEDA it is, because it talks about an organization. If they send information out for processing, the organization remains responsible for it, even if they've handed it off to somebody else for processing.

The scenario you just described is not addressed in the Privacy Act. If there were a requirement that the government institution implement safeguards to protect the information they collect, part and parcel of it is that they make sure of the security of that information wherever it goes, which would make the public body accountable, I would expect, for the information in the hand, for example, of an outsourced processor.

Mr. Brian Murphy: Would a contract for the service delivery not impose on the private service deliverer the same obligations as the parent—the government—has?

Mr. David Fraser: Yes, and that is included in Treasury Board guidelines with respect to outsourcing or third-party processing of personal information.

Mr. Brian Murphy: This leads me to another question about crown corporations. A number of MPs are fighting battles with the Canadian Border Services Agency with respect to reports on customs services at airports and so on. That is again too example-specific, but the scope of either the Privacy Act or PIPEDA toward crown corporations leaves them in a sort of no man's land sometimes. Are they explicitly covered by the Privacy Act, or are they occasionally covered by PIPEDA? Is there a gap there?

● (1720)

Mr. David Fraser: There is the potential. Under the Privacy Act, government institutions come into coverage of the Privacy Act by being listed in the schedule, so if there's a crown corporation that is not listed in the schedule, it is not subject to the Privacy Act. PIPEDA begins to apply if you're a federal work, undertaking, or business, or are engaged in commercial activity. Then it says that if you are subject to the Privacy Act, you're not in.

So you can have a crown corporation that is not engaged in commercial activity and that is not listed in the schedule which is not covered by any privacy legislation. I can imagine that happening.

Just to bring your two scenarios together, we have an increased number of programs being delivered jointly by the federal government and the provincial governments—the Canada-Ontario Business Service Centre, Canada/Nova Scotia Business Services Centre, and the like—and the provincial legislation and the federal legislation don't specifically delineate who is responsible for the information when it's collected by a contractor on behalf of both governments.

Mr. Brian Murphy: Do you see any problem with setting up the Canadian equivalent of a centre for disease control as they have it in the United States? Obviously it is very well publicized. In Canada it is patchwork: this hospital reports its outbreak of flu, or whatever. Do you see these two acts prohibiting that sort of setup because of the confidential nature of...?

Mr. David Fraser: Not particularly. Pretty well every province has public health legislation that explicitly overrides or requires the reporting of communicable diseases. Just about every piece of privacy legislation in Canada says you can disclose information without consent if you legally have to. They're designed to hopefully fit together.

Mr. Brian Murphy: I didn't know that.

Thank you very much.

The Vice-Chair (Mr. David Tilson): We have Mr. Hiebert, Mr. Wallace, and Madame Lavallée.

We'll do our best, Madame Lavallée. We'll see how these other fellows do.

[*Translation*]

Mrs. Carole Lavallée: I would be pleased to do so if there is some time remaining. If not, that is allright.

[*English*]

The Vice-Chair (Mr. David Tilson): Mr. Hiebert.

Mr. Russ Hiebert: Thank you, Mr. Chair.

You talked in your earlier comments about the importance of foreign countries providing written, formal, detailed, and public documents under the agreements we have with other countries. We had CSIS and the RCMP here, and they made the statement that sometimes you simply can't do that. Sometimes these countries won't agree to having public documents or written documents. Sometimes it's simply not timely: the nature of the potential emergency or concern is such that you can't go through an iterative process of negotiation and drafting and that sort of thing.

How would you respond to those concerns? Your recommendation is that their worst fear would become reality: that they would have to have written, formal, detailed, and public documents with foreign countries.

Mr. Gregory DelBigio: Without knowing the specifics, it's difficult to comment upon what countries would not agree and the reasons they might not agree, but that would need to be carefully assessed against the requirements of accountability. So it is certainly something that would be of interest if there are any large numbers of democratic countries that would be refusing to enter into such an agreement.

On the other hand, would it equally be of interest if this were simply one or two isolated incidents? More information is needed. And on the issue of timeliness, again, what the law attempts to achieve is a framework of general guidance. Will it cover each and every situation? Perhaps not, but the law attempts to achieve the best balance it can using the words that are available to us to create this general framework.

Mr. Russ Hiebert: I understand your point. I think the point they're trying to make is that the vast majority of nations in the world do not have privacy legislation like we have or anything comparable, so there would be numerous examples of countries that might just throw up their hands and say "Sorry, we're not interested." Then when you have to debate whether we fulfill the Privacy Act or whether we protect and secure Canadian citizens, it's not a difficult debate in their minds. So I think there is more discussion that needs to happen on that front.

I want to draw to your attention—and perhaps you're not familiar with this particular decision—that there was a case, Murdoch v. Canada, specifically the RCMP, in 2005, where the RCMP wrongfully disclosed personal information about an individual to their employer. Mr. Murdoch took this case to court, and the court found that the Privacy Act did not allow for Mr. Murdoch to claim damages for this breach of privacy.

Do your recommendations suggest that individuals like Mr. Murdoch should have an opportunity to seek damages under these circumstances?

Mr. David Fraser: The specific recommendation that deals with the ability to go to the Federal Court is the commissioner's recommendation 2, on page 6. It's not a model that is designed in order to seek damages or to seek compensation. It's a model that is intended to make sure that those within government organizations or government institutions can be compelled to follow the particular law. It's not based on a model of damage compensation or otherwise, and it's not a point we spent any significant amount of time on.

Mr. Russ Hiebert: So you're not suggesting that it be incorporated into the changes, that there be an opportunity for Canadians, where they felt it necessary, to find redress from the courts. I know it's not in your recommendations, but in addition, your own thoughts are not that we should have such an amendment?

● (1725)

Mr. David Fraser: No, certainly it wasn't anything that was identified as a priority with respect to reforming the Privacy Act, so it wasn't something any particular attention was focused on.

Mr. Russ Hiebert: Fair enough.

Mr. Chair, I'll pass the balance of my time to the next member.

The Vice-Chair (Mr. David Tilson): You have no time.

Mr. Wallace.

Mr. Mike Wallace: Thank you, Vice-Chair.

I'm happy to share with Madame Lavallée if there are a few minutes left.

When I first got here, I moved a private member's bill to deal with a database for missing persons. There isn't one that exists federally. There is some semblance of that provincially. There are some provincial jurisdiction issues.

One of the things that surprised me was that there were privacy issues, in a sense, around those who didn't want to be found and have gone missing because they're hiding from an abusive relationship, for example. But for the vast majority.... As an example, there's an individual right now in Hamilton who is pushing hard that she has DNA of a missing son that could be used to maybe find him. Otherwise you have to rely on information or go to different morgues across the country to see if the individual might be there, and so on and so forth.

It doesn't solve all the problems, but my question to you today would be, based on the Privacy Act, since you have some experience with it, and these recommendations that you have in front of me, do you foresee that they would in any way hinder my goal of adding a missing persons database to what is there already?

As you know, there's a database for criminals, sex offenders and a number of others. I want to have a more positive database that individuals can access if they have DNA of individuals who are missing.

Do you foresee, from the association's point of view or any of these recommendations, that there are any issues dealing with that concept?

Mr. David Fraser: Are you proposing a database...if the relatives of missing people can have the particulars of the individuals put in the database?

Mr. Mike Wallace: I'll give you an example. Let's say my daughter goes missing. The rule of thumb is that most missing people are found within a few days or a few months. Then what you'd call missing long term is after a year. One way or another, 80% are found within the year.

Let's say I have a brush with my daughter's hair in it. I want to take it to the RCMP for the missing persons database. I want them to do a DNA analysis of my daughter's hair. If my daughter is found at a crime scene, or in a farmer's field, or in a morgue, I'd like to be notified so that I can put closure to my family's tragedy.

There are some issues here. For instance, men or women can leave abusive relationships and assume different names and so on and so forth. So if the person is found alive—this is in my bill—they have to give permission to the person who's been looking for them. But if the person who has been found is deceased, the family members are notified.

Does your organization have any view on that? Does anything you're recommending in here on the Privacy Act—I know this will have to be a quick review—affect that at all, do you think?

Mr. David Fraser: Hypothetical examples are almost never as simple as they seem on the surface.

As for a quick review of our recommendations and whether I see them having a significant impact on that, no, I don't.

Mr. Mike Wallace: Thank you.

I'll share whatever time I have left with Madame Lavallée.

The Vice-Chair (Mr. David Tilson): Well, we can see the clock. You have not much time.

Mr. Mike Wallace: Sorry.

[*Translation*]

Mrs. Carole Lavallée: Do I have one or two minutes?

The Vice-Chair (Mr. David Tilson): Two minutes.

Mrs. Carole Lavallée: Allright. I had some one, two and three-minute questions. I'm going to choose a question that will take only one minute.

In your brief, you did not refer whatsoever to the destruction of personal information. The current act does not say much about this issue. Section 6(3) is the only place where reference is made to the destruction of information. It reads as follows:

> (3) A government institution shall dispose of personal information under the control of the institution in accordance with the regulations and in accordance with any directives or guidelines issued by the designated minister in relation to the disposal of that information.

I did not consult the English version, but in the French version, the word "retrait" is used. I find it odd that this word is used in the French version in order to refer to the destruction of information. Not much reference is made to this issue and there is no obligation, as is the case in the Personal Information Protection and Electronic Documents Act, to ensure that documents are destroyed in accordance with the rules. A great deal of information is leaked when it is being destroyed.

What are your comments on this issue?

● (1730)

[*English*]

Mr. David Fraser: I hope I have fully understood your question.

We have put in a recommendation with respect to safeguarding personal information. An important aspect of safeguarding information is to make sure that it's safely and appropriately destroyed when it's no longer needed. That also goes hand in hand with the necessity requirement, that information should really only be collected and used if it's necessary. If it's no longer necessary, it should no longer be kept. At the end of that, principles of safeguarding would require that information to be destroyed.

PIPEDA also permits that information to be made anonymous, to have all the identifiers taken out. Statistical information can be very useful at the end of the day, so you're not throwing out all the value of the information, you're just removing the personal identifiers, which is analogous to its destruction. But destruction is an important part.

The Vice-Chair (Mr. David Tilson): Thank you very much, sir.

The Canadian Bar Association has done well. We always appreciate the representatives who come and give us their wisdom, and you two are no exception. Thank you very much for coming.

The meeting is adjourned until Thursday at 3:30 in this room.

Published under the authority of the Speaker of the House of Commons

Publié en conformité de l'autorité du Président de la Chambre des communes

Also available on the Parliament of Canada Web Site at the following address:
Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante :
http://www.parl.gc.ca

The Speaker of the House hereby grants permission to reproduce this document, in whole or in part, for use in schools and for other purposes such as private study, research, criticism, review or newspaper summary. Any commercial or other use or reproduction of this publication requires the express prior written authorization of the Speaker of the House of Commons.

Le Président de la Chambre des communes accorde, par la présente, l'autorisation de reproduire la totalité ou une partie de ce document à des fins éducatives et à des fins d'étude privée, de recherche, de critique, de compte rendu ou en vue d'en préparer un résumé de journal. Toute reproduction de ce document à des fins commerciales ou autres nécessite l'obtention au préalable d'une autorisation écrite du Président.