House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 031 • 2nd SESSION • 39th PARLIAMENT

EVIDENCE

Thursday, May 1, 2008

Chair

Mr. Paul Szabo

Standing Committee on Access to Information, Privacy and Ethics

Thursday, May 1, 2008

● (1530)

[*English*]

The Chair (Mr. Paul Szabo (Mississauga South, Lib.)): Good afternoon, colleagues.

Our order of the day is Privacy Act reform.

Today we have as our witnesses, from the Treasury Board Secretariat, Mr. Ken Cochrane, who is the chief information officer, and Mr. Donald Lemieux, who is executive director for information, privacy, and security policy.

I understand Mr. Cochrane has an opening statement, of which you have a copy.

The members have asked me about whether or not the Treasury Board representatives had received a copy of the document with regard to the recommendations for consideration with regard to Privacy Act amendments. They are aware of them, but we have to be a little bit careful in our expectations because of the role and responsibilities of Treasury Board in this regard. I think Mr. Cochrane is going to address that.

Mr. Cochrane and Mr. Lemieux, welcome, and please begin.

Mr. Ken Cochrane (Chief Information Officer, Treasury Board Secretariat): Thank you very much, Mr. Chair, and good afternoon.

My name is Ken Cochrane, and I am the chief information officer of the Government of Canada.

Today, as the chair indicated, I am accompanied by Mr. Donald Lemieux, who is the executive director of the information and privacy policy division of the Treasury Board Secretariat, so the subject expert in this particular area within the secretariat.

I'd like to begin by thanking the committee for this opportunity to discuss the policy role that the Treasury Board Secretariat plays with respect to privacy across the Government of Canada. We have been invited by your committee to offer our knowledge of the policy on privacy protection and the privacy impact assessment policy, for which the Treasury Board Secretariat is the lead department. Therefore, I'd like to take a few minutes to provide an overview of the Treasury Board Secretariat's role in supporting the policy instruments we are responsible for.

First, it's important to note the shared responsibility of the Treasury Board Secretariat, the Department of Industry, and the Department of Justice in the area of privacy protection. In this respect, the policy on privacy protection and the privacy impact assessment policy are under the responsibility of the Treasury Board Secretariat. These two management policies support the Privacy Act. The Privacy Act itself falls under the responsibility of the Minister of Justice, and the Personal Information Protection and Electronic Documents Act, PIPEDA, which the Privacy Commissioner has previously discussed with the committee, is administered by the Minister of Industry.

Heads of institutions are responsible for ensuring that their organizations comply with management policy and legislative requirements.

So the President of the Treasury Board is the Minister designated under the Privacy Act with the responsibility for developing and issuing management policies and guidelines to ensure the effective administration of the act itself. The Treasury Board Secretariat supports the president in this role by developing policies and guidelines and by providing ongoing training and support to the access to information and privacy community in government.

It's important to note that the head of each institution is responsible for protecting personal information under their control and adhering to management policies and this legislation. Detailed information on privacy management policy instruments can be found in the manual that we have provided to the committee members.

I'd like to provide you with a little more information on the privacy policies that fall under the Treasury Board Secretariat's responsibility. As members of the committee may know, the government is going through an extensive renewal of its management policy suite, and this renewal includes our privacy policy instruments. There are two privacy policies issued by the President of the Treasury Board to support the Privacy Act itself: the policy on privacy protection, and the privacy impact assessment policy.

The policy on privacy protection replaces the former policy on privacy and data protection. It was recently revamped to reflect changes made through the Federal Accountability Act. This policy aims to ensure a number of things: first, that sound management practices are in place for the handling and protection of personal information; that clear decision-making and operational responsibilities are assigned within government institutions; that there is consistent public reporting through annual reports to Parliament, statistical reports, and the annual publication of Infosource, produced by the Treasury Board Secretariat; and that there is identification, assessment, and mitigation of privacy impacts and risks for all new or modified government programs and activities that use personal information.

The privacy impact assessment policy itself is the second management policy we are responsible for, and it was implemented in 2002. Privacy impact assessments assure Canadians that privacy principles are being taken into account when planning, designing, implementing, developing, and changing programs and services that raise privacy issues. The results of government privacy impact assessments are communicated to the Privacy Commissioner and to the public. We are currently reviewing this policy and we are working in close collaboration with the Office of the Privacy Commissioner on this matter. We expect our review will be completed within this fiscal year.

To go on with the role of other institutions, while the secretariat plays an important role in establishing policies and guidelines and providing guidance to the ATIP community, heads of government institutions are ultimately responsible for personal information under the control of their respective institutions. They are responsible for ensuring that their organizations comply with all the Treasury Board Secretariat's management policy requirements. And institutions are assessed annually on their compliance through MAF, the management accountability framework, which I am sure you are familiar with.

Specifically, for privacy-related management policy instruments, the responsibility of implementing requirements within institutions is generally delegated to ATIP coordinators within departments. Treasury Board Secretariat is the leader of the privacy community across government.

● (1535)

Given the importance of the mandate of the ATIP community, the Treasury Board Secretariat has adopted different measures to help federal institutions adhere to the policies regarding privacy. For example, Treasury Board Secretariat provides ongoing training to the ATIP community. We do this through a variety of means, such as developing training material and hosting training sessions to ensure members of the community are informed of the latest policy developments; by distributing guidance documents to ATIP practitioners; by holding regular community meetings to share issues of interest and best practices and advise the community of any changes to the policy; and by responding to questions from ATIP practitioners who require assistance and advice on the interpretation of our policies.

Finally, the Treasury Board Secretariat publishes the annual InfoSource bulletin that contains statistics of requests made under the Access to Information Act and the Privacy Act, and summaries of Federal Court cases of relevance to the interpretation of the acts.

Mr. Chairman and members of the committee, as you know, the government is strongly committed to the protection of individual privacy rights. Our policy instruments aim to support legislation that is passed through the House of Commons by parliamentarians on behalf of Canadians. These policy instruments are robust and are taken very seriously by government institutions. I'm confident that the privacy policies strengthen the rights of Canadians in regard to the sound protection of their personal information.

As this committee continues to study the Privacy Act, the Treasury Board Secretariat will await direction set in law by Parliament.

Mr. Chairman, this concludes my remarks. Mr. Lemieux and I would be very pleased to answer any questions from the committee.

The Chair: Thank you very much, Mr. Cochrane.

Very briefly, section 71 of the Privacy Act sets out the duties and responsibilities of Treasury Board. Can you give us a very brief assessment of the state of the union, as it were? I think the committee would probably be very interested in the areas in which there should be some attention or concern.

● (1540)

Mr. Donald Lemieux (Executive Director, Information, Privacy and Security Policy, Treasury Board Secretariat): With regard to section 71 of the Privacy Act, it basically divides the responsibilities when it comes to regulations. For example, you're looking at certain regulations the Treasury Board Secretariat would be responsible for.

With regard to, as you put it, the general state of the union when it comes to the Privacy Act, although it's one of the first pieces of legislation that's been around, it seems to have weathered the time to the extent that it is still vibrant. Certainly it's been supplemented by the Treasury Board Secretariat in the policy suite renewal exercise Mr. Cochrane referred to. The policy suite renewal in general is part of the action plan under the Federal Accountability Act in terms of strengthening some of the measures. For example, we added a number of institutions under the Privacy Act. Seventy institutions were covered under the Access to Information Act as a result of the FAA, but to do so we also had to cover those institutions under the Privacy Act.

It's maybe not as obvious, but if you look at the way the two acts hang together, the Access to Information Act and the Privacy Act, the definition of what is personal information is in the Privacy Act, so we had to include those institutions in the Privacy Act. So the span now covers approximately 250 institutions.

The Chair: Okay, maybe we'll get a little bit more on these kinds of matters.

I have Mr. Hubbard, Madame Lavallée, and then Mr. Wallace.

Hon. Charles Hubbard (Miramichi, Lib.): Thank you, Mr. Chair, and good afternoon.

In terms of the work you do in this area, how big is your staff? How many people work directly with you in providing this service to other departments?

Mr. Ken Cochrane: Mr. Lemieux may go into more detail, but his team is about 35 people overall. They support both the privacy elements and the access to information elements on both sides, so it's a mixed team supporting both of these areas. A lot of that, of course, is supporting, as I was indicating, training and answering a lot of questions from the community, in addition to developing many of the instruments and the policy instruments.

Hon. Charles Hubbard: In your brief you indicated that a number of programs were ongoing. You indicated, for example, one by the end of the year. How many initiatives do you have? The Federal Accountability Act has really been a big factor in what you're trying to do. Do you have a timeline for the objectives you have, where point A is going to be done by July of 2008, and the other by the end of 2008, and so forth? How would you define the major ones, and when would the completion dates be for each of them?

Mr. Ken Cochrane: Maybe I'll start that, and once again I may turn to Mr. Lemieux.

We've broken the role out of the policy work, and it's all part of policy suite renewal, as I'm sure you're well aware. A big part of policy suite renewal was to simplify policy so departments could execute it much more effectively.

In phase one—which really just ended in April 2008, so we had a very tight timeframe—we renewed the access to information and protection of privacy policies, so those policies are now in place and renewed. And there is a directive now on social insurance numbers that is currently in place.

What we're calling phase two takes us from current until April 2009, and it will look at establishing a number of directives that are mandatory instruments under the policy. There will be a directive on the administration of the Privacy Act that will help departments understand how to actually manage the work they must do under this, and there will be a directive on privacy impact assessments. It's currently a policy, but we're changing it to simplify it and put it right under this area. It will also be done in this timeframe.

There is a privacy management directive, and a directive looking at the administration of the Access to Information Act. And there is work that we're doing—and now I'm into a bit of a broader sphere—on duty to assist, which is probably more on the Information Commissioner's side. That is an important piece of the dialogue that needs to take place between us and the Information Commissioner and the rest of the town. I describe that because it's part of an integrated plan, and there are a number of things under way right now with the team.

Hon. Charles Hubbard: Under the Access to Information Act, it seems that the press in fact were quite concerned recently when we decided to take this area of study instead of access to information. It appears, anyhow, that under the Access to Information Act the press and a great number of members of Parliament and the public are complaining that access to information has become a very complicated issue, and often the deadlines under the access to information program are not met.

In terms of your work, are you in any way impeding the work that is being done by that office, the Access to Information Office?

● (1545)

Mr. Donald Lemieux: Mr. Chair, just to make sure I understand the question, in terms of our work we provide policy advice and support the administration of the program throughout the 250 institutions. A large component of that is the training and development of the ATIP personnel, the people who are on the ground answering those requests.

Our responsibility is to make sure that the community understands what their roles and responsibilities are.

As I'm sure you will appreciate, we have added 70 new institutions as well, which is quite important. We were 180 institutions, and we're now 250, so we've added a considerable number. We're putting a lot of effort into doing that, under both the Access to Information Act and the Privacy Act. We do our best to support the institutions in streamlining processes.

If I can just add to something that Mr. Cochrane mentioned earlier, about making it easier for institutions in some of the work we do, one of the big efforts that we have in our division is to put together InfoSource. That's a huge publication, and it's much larger now because we have all these new institutions. One of the things we're looking at is to make it much easier for institutions to do those updates. We're trying to facilitate their jobs by doing that.

As well, because we've grown to support the ATIP community, we have established call centres, and we have a website that we're using to facilitate the work that's done. We're doing everything in our power, within our responsibilities and within our roles, to support the community so that they can deliver the service, duty to assist being a big one that Mr. Cochrane mentioned.

Hon. Charles Hubbard: When you indicate this to this committee, in no way are the new guidelines or anything tied to the Federal Accountability Act impeding the problems that the Information Commissioner is having in getting his work done?

Mr. Donald Lemieux: Impeding? Not at all. In fact, when we're doing the policy suite renewal work that we're doing we are in lockstep with both commissioners moving forward.

For example, we have a working group where there are two representatives from the Information Commissioner's office; we have an ADM committee, and there are representatives from the commissioner's office. We have bilateral meetings with them throughout that process, and that's access and privacy.

We're quite conscious when we do something that it supports the program, and we work with both commissioners.

The Chair: Now we'll go to Madame Lavallée, *s'il vous plaît*.

[*Translation*]

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

Thank you for enlightening us on how the Personal Information Protection Act is implemented. It's more that component that interests us, at least today. We would have preferred to study the Access to Information Act first.

Mr. Lemieux, you referred to the ATIP community, that is to say the access to information and privacy community. In concrete terms, are access to information officers the same as privacy officers?

Mr. Donald Lemieux: In most cases, yes, although that depends on the institution. For example, a large institution may have one office for access to information and another for privacy. That way of doing things may be practical for a department with 20,000 employees, but, on the whole, the office of each institution combines access to information and privacy. There are benefits to that. The two acts are similar and must often be weighed, for example, when an exemption is sought for personal information.

Mrs. Carole Lavallée: They are the same individuals.

● (1550)

Mr. Donald Lemieux: On the whole, yes.

Mrs. Carole Lavallée: You're right: the Access to Information Act and the Privacy Act are like the Chinese yin and yang. For some people, however, they must make it hard to make decisions. For example, one senior official came here and had a lot of trouble providing information in response to an access to information request. She said that she herself is very concerned about the confidential nature of the information. She was the access to information coordinator.

It seems to me that having to handle two acts creates difficulties for officials. Wouldn't it be better to separate those duties? There are two commissioners. Why isn't it the same for the employees?

Mr. Donald Lemieux: In different jurisdictions, that can operate differently. There are always advantages and disadvantages. I'm a former coordinator. So I've had—

Mrs. Carole Lavallée: —existential angst.

Mr. Donald Lemieux: Yes, exactly. Some issues are quite difficult. As director general responsible for access to information and privacy, I can weigh the pros and cons. When I make a decision concerning access to information. I'm very much aware that it can have repercussions. It's really balanced. Without knowing the exact reason why the coordinator made that comment, I can say that certain decisions are difficult. We encourage those people to come and see us. There are also teams that can talk with their legal department. It's working quite well on the whole.

Mrs. Carole Lavallée: Are coordinators more inclined to censor information?

Mr. Donald Lemieux: That's very hard to say without talking about a very specific case. Coordinators will understand their role and the exceptions they have to apply or what we call exclusions, like Cabinet confidences. The complaints mechanism of the Commissioner's office can be used. So if a coordinator's freedom of action is too restricted, in that case, the Commissioner will intervene in accordance with the act.

It's the same in the case of privacy. Where it really becomes confusing... In an ideal world, a file contains the personal information of a single person, but if it contains personal information on more than one person, that complicates matters.

Mrs. Carole Lavallée: Perhaps in most cases it's information that an access to information coordinator wants to protect, but that isn't necessarily personal.

You know the nature of the exclusions, including national security. For an official, isn't it more tempting to censor more rather than less? Unless it's a very sensitive file like the report on the human rights of Afghan prisoners, which rarely occurs, it seems to me that officials have to weigh matters quite a bit more in order to be sure of avoiding problems. However, if they side more with the public and are more inclined to provide it with the information, as the public is entitled, they may have problems.

Mr. Donald Lemieux: Once again, I can only talk about my experience. I can say that it was helpful to play both roles. When I explained to senior management officials their responsibilities under both acts in a specific case, I was well equipped to do so.

There definitely can be more difficult cases, but the act has been around for 25 years, and I think that it's working quite well on the whole.

● (1555)

Mrs. Carole Lavallée: How much time do I have left, Mr. Chairman?

[*English*]

The Chair: You have 30 seconds.

[*Translation*]

Mrs. Carole Lavallée: Thank you very much.

[*English*]

The Chair: Mr. Wallace.

Mr. Mike Wallace (Burlington, CPC): Thank you, Mr. Chair.

And thank you, gentlemen, for joining us today. I'll try to go fairly quickly through my questions.

In your presentation you talked about shared responsibility: the Privacy Act is the Department of Justice, PIPEDA is Industry Canada, the Treasury Board is another. Would it be better to be all under one ministry? Are you able to give us that kind of response? Does it cause any difficulties from an administrative point of view at the bureaucratic level?

Mr. Ken Cochrane: Meaning that the two acts being under—

Mr. Mike Wallace: We've really got three departments. You even mention here that you've got three areas that are responsible for different things. Do you have any issue with that?

Mr. Ken Cochrane: I don't think so, because fundamentally we're looking at the Privacy Act, which is with the Department of Justice, and the Access to Information Act, which is with the Department of Justice. PIPEDA, which really focuses outside of government, is with Industry Canada, and I believe that's a rational place for it to be. And we sit in the centre looking inside the government, so I don't think we have any difficulties there.

Mr. Mike Wallace: Okay, I appreciate that.

You say the Treasury Board Secretariat provides management policy support to the Privacy Act. When you say "support", what do you mean by that? Does that mean that if I have a problem and I'm working in another department, I call you and you give me advice? Or do you provide manuals on how to do things? What do you mean by "support"?

Mr. Ken Cochrane: Really what we're looking at, then, is this. Here is the act; it's been established in legislation. The people in the Treasury Board Secretariat in the different policy areas—so in ours in this particular case—take that legislation or that act and interpret it in terms of what the actual administrative rules will be. So we do some translation of that so departments can act appropriately according to the act.

Mr. Mike Wallace: And you provide that to the departments.

Mr. Ken Cochrane: We provide that to departments along with.... So when we say "support", it goes all the way from not only providing it, but publishing it, providing tools, easy access tools, training, and a help desk.

Mr. Mike Wallace: So you're used to doing it all the time on the support side.

The Privacy Commissioner has presented us with some suggestions in terms of improvements, and I think there are ten or eleven recommendations. As a group we're working on this. From the Treasury Board point of view, should that come from the President of the Treasury Board in terms of suggestions for changes, or have you as the administrative staff on this looked at things you'd like to recommend to this committee on changes to the Privacy Act to make it easier for you to do your job or to support the system?

Mr. Ken Cochrane: I'm just going to just turn that over to Mr. Lemieux.

Mr. Donald Lemieux: First of all, I think I mentioned we just got the recommendations....

Mr. Mike Wallace: From her, I know, but have you, as the Treasury Board, been looking at this at all from the point of view that during this review, which may last a few weeks...? Who would we call on from the Treasury Board to say "Okay, you guys support this. You see where the rubber hits the road on these issues, often, in your support groups. Do you have suggestions for us?" Has that process taken place in the Treasury Board?

Mr. Donald Lemieux: Not to the extent that I think I understand from your question. When I look at these recommendations, at the outset I need clarity about what exactly they are getting at. I think we're still at the discovery stage in terms of the scope. I know there were a few that were specifically mentioned, such as Madam Stoddart mentioned about the Treasury Board Secretariat and some of the stuff we've done already in policy.

Mr. Mike Wallace: So you'd be comfortable, then, if we gave you some time and called you back? Would you be able to look at that in the next month or so? Is this a political thing, or are we okay in asking you what you think?

Mr. Ken Cochrane: It's an interesting space for us, because some of it is in the act, and that's the prerogative of Parliament to make decisions on what they want to incorporate.

But where we spend our time with the commissioners—and we have a good relationship with the commissioners because of our role—is looking at the practicality of a decision that might go into a piece of legislation. If we do that, it may sound good, but is it practical? Can the community manage it effectively? From that perspective, there's likely a role we could play in providing feedback.

Mr. Mike Wallace: That's a perfect segue to the area I wanted to talk about today, which I probably only have a couple of minutes left to do. With respect to the privacy impact assessment reports that now exist but are not part of legislation, would you consider them voluntary, or are they a requirement but not legislatively required?

● (1600)

Mr. Ken Cochrane: They are a mandatory requirement because we've established that as a directive under management policy for the Government of Canada. The reason I say they are mandatory is that these instruments the secretariat has put in place are mandatory for heads of institutions to follow. In addition, as you well know, we determine whether they're following them through vehicles such as the management accountability framework. So we look very closely at their compliance.

Mr. Mike Wallace: So the head of the department does this privacy assessment when there's a change in the program, or a new program. What happens to that information for that report? Does that reside with TB? Does it stay with their department? What actually happens with that information? And if you're not happy with it in terms of following the Privacy Act, based on your interpretation, what's the recourse? What happens to these reports?

Mr. Donald Lemieux: Maybe I could address that, Mr. Chairman.

If a government institution is on a project that has privacy implications, then they would first prepare a privacy impact assessment—a quick review that will service any privacy issues. Obviously there are files that would immediately suggest that, so they ask some basic questions. Then they will consult the Privacy Commissioner so the Privacy Commissioner is immediately engaged in the privacy issues related to that specific program.

We are working with the Privacy Commissioner and departments right now on how to make it better. The policy came into effect in 2002, and we're looking at a more streamlined process. We want to avoid any delays. We want to be much more efficient in doing these privacy impact assessments and developing templates—that useful tool that institutions will need to help identify, for example, horizontal issues.

Mr. Mike Wallace: Have you been discussing in these meetings the need for it to be legislated or not?

Mr. Donald Lemieux: Because of the nature of the mandate of the policy suite renewal, it's limited to the policy realm. And again, we are working in lockstep with the commissioner on this.

Mr. Mike Wallace: I appreciate that. Thank you very much.

Thank you, Mr. Chairman.

The Chair: Mr. Pearson.

Mr. Glen Pearson (London North Centre, Lib.): To Mr. Cochrane, when the Privacy Commissioner was here, she thought it would be a good idea to have a legislative requirement for government departments to demonstrate that they need to collect information. It was interesting when she said that. I would like to know what procedures are currently in place when you do that. Also, what is your system for notifying people that you need this information?

Mr. Ken Cochrane: We understood that requirement was suggested. It is in fact a requirement of the current policy. Mr. Lemieux is just pulling out that piece; perhaps you want to refer to it. I think it will answer the question. But it is well understood by departments that they must follow through on that step initially.

Mr. Donald Lemieux: Just in general terms. It's in chapter 2-2. We provided the committee with a binder that has the guidelines. I appreciate that there's quite a bit.... It says something about the information that we give our ATIP community, I guess. So it's chapter 2-2, page 1. It says:

> The legislation states that government institutions shall not collect personal information unless it relates directly to an operating program or activity. The policy requires that institutions have administrative controls....

It goes further. The policy requires that institutions have administrative controls in place to ensure they do not collect any more information than is required. And it goes on.

So there is already something in the policy in addition to the legislation, and again, as Mr. Cochrane mentioned, policy is binding on these government institutions to limit the collection of personal information when they're starting off on a new program.

Mr. Glen Pearson: Why, then, is she calling for a legislative requirement if you're saying it's already in there? I'm just trying to understand.

Mr. Donald Lemieux: I haven't had a discussion, nor have any of our officials, on why they feel that it should be there. Perhaps she's looking at other jurisdictions, or she's had discussions. I really can't say.

● (1605)

Mr. Glen Pearson: The legislative requirements that you just read out to us from your binder, are they applied—

Mr. Ken Cochrane: I should just clarify. They're policy requirements.

Mr. Glen Pearson: I'm sorry. You're right, thank you.

Are they applied equally across all the departments of government on this issue?

Mr. Donald Lemieux: It's binding on every institution, all 250 now, to do that.

Mr. Glen Pearson: To what degree are they monitored by the Treasury Board to make sure that's done?

Mr. Donald Lemieux: I think the way the mechanism is done—the watchdog, the mechanism, the framework that was set up in the legislation.... There is what they call the four-to-eight. The Privacy Commissioner has audit powers, and she and her staff can come in and do an audit of whether or not they're managing four-to-eight. That's on the collection—which is what I referred to—and the use and disclosure of personal information. So the way the regime in the act was structured is that the commissioner, who has audit powers, can go in there. It can be done also based on a complaint from an individual that it's not being done properly.

So that is the mechanism. The act did not set up a situation where both Treasury Board and the Privacy Commissioner would have the same role of auditing. They specifically gave the Privacy Commissioner those audit roles, subject to, of course, complaints by individuals, which I mentioned.

Mr. Glen Pearson: Can you compare for me, then, the policy that you have with PIPEDA and the collection of information? Are they comparable?

Mr. Donald Lemieux: Unfortunately, I'm not an expert on PIPEDA because it's Industry Canada legislation. It's not the legislation I work with. I want to be quite frank with you that I'm not the expert to be able to do that. But the regime that they set up in PIPEDA is different from what's in the Privacy Act. I can't really evaluate it. That would require a detailed study. I'd hesitate to do so without having done that.

Mr. Glen Pearson: That's fair enough.

The Privacy Commissioner was saying that she feels there's a need, when information is collected, for it to be done in as open and transparent a way as possible. I'm not saying she was implying that it wasn't being done that way, but can I ask what your policies are on that or how you pursue that?

Mr. Donald Lemieux: Again, Mr. Chairman, I haven't had the benefit of the exact context in which she said that. She may have seen that.... I'm not even aware that she's reported on that in an annual report, although she may have.

I have no particular knowledge that there's a shortfall there or that there's something she has observed. Certainly, as I said, we have regular meetings. There's nothing specific that has been brought to my attention to say that is an issue—and I tend to have regular meetings.

Mr. Glen Pearson: Well, what specifically do you have that keeps a transparent accountability mechanism? I'm digging a bit here, I know, but I'm just trying to understand where she's coming from.

Mr. Ken Cochrane: Mr. Lemieux will correct me, I'm sure, but I'm thinking that when we look at this, part of it is that the privacy impact assessment to some degree marries in with this process. So although you're collecting information, part of it is impacting it, and that's a very transparent process. A report is produced, a serious assessment is done. It is published on their website. It is made available to the commissioner. That's a very public part of the process, and I believe that's done as they establish any new information holdings.

Mr. Donald Lemieux: One thing that I might add that I probably should have mentioned earlier is the tie-in it has with the InfoSource. That's the publication I referred to. I always say it's one of the most important parts of the legislation, because you can have all the rights you want, but if you don't know what type of information the government holds on you, then it's a sort of hollow right. In InfoSource there are what they call “personal information banks”, and there is a lawful responsibility on behalf of the heads of the institutions to describe their personal information banks. So that's the transparency element that the public will be able to see.

The Chair: We'll now move to Mr. Allen.

Mr. Mike Allen (Tobique—Mactaquac, CPC): Thank you, Mr. Chair.

Thank you, gentlemen, for being here today.

I've been a longstanding member of the committee, and there are a few things that intrigue me about your presentation, especially on current issues on privacy.

First, Mr. Cochrane, your role is CIO. What intrigues me, with respect to the policies, is identification assessment and the mitigation of privacy impacts and risks. Given all the government information systems we have, the majority of which are disjointed, what kind of risk assessment has been done on those systems? How does that fit within the new Privacy Act? How are you trying to deal with the number of information systems that are collecting information?

● (1610)

Mr. Ken Cochrane: That's a very good question.

It's one of the challenges of the role of CIO. There are a number of different groups within the CIO branch of Treasury Board Secretariat. Mr. Lemieux has the privacy and access to information people. We have a group that focuses on what we call enterprise architecture. We have another group that focuses on information management. You can see very quickly that there are overlapping and complementary elements.

The people who look at enterprise architecture draw a map of what the government looks like. They look at whether there is common information and try to create a map so that when we move forward and add new systems, processes, or programs, there's a good understanding of the ability to reuse and affect information that already exists. That's a very important discipline and one that we follow very closely. They work in close cooperation with Mr. Lemieux's area.

The information management people, on the other hand, develop basic models of what information should look like in government. If we hold human resources information in 60 different institutions, we should follow a standard. And if we're looking at geomatics information, it should follow a standard so we can look at it in a coherent fashion and understand it overall. I think that really supports the work Mr. Lemieux does as people change information or modify information. It allows us to look at things holistically.

One of our most important assignments in the chief information officer branch is to establish standards for government operations. When you're in unique business lines, that's fine. But when you're in business lines where information crosses over, we establish common standards so we can understand the information much more effectively.

Mr. Mike Allen: We continue to hear these horror stories. You believe that all this information is secure, then someone steals a laptop, and it's gone. Then you hear that people's personal information or social insurance numbers were on it.

What kinds of safeguards do you anticipate putting in place to make sure that the assets are protected as well? Are there provisions for that?

Mr. Ken Cochrane: This is where privacy starts to drift into security. We also have the security policy for the Government of Canada. When we look at security, I'd say there are three main areas. One is the physical security of our buildings and facilities. The second is personnel security and screening, because those are all factors in the loss of information. The third is IT security. That whole policy area really deals with that.

When you look at IT security, specifically, first of all, you want to make sure your facility is sound. The security policy with respect to facilities very much deals with how you need to secure a facility so that people can't go in and take things.

In the case of laptop computers and mobile computing, the information technology security part deals with the way you need to store information if you are going to be mobile. There are very specific rules in place as to what should be on mobile equipment. If it's there, you need to encrypt it and protect it.

If you're using mobile equipment to gain access to government, there are very specific rules on how you need to access government services through secure channels and secure networks. There's a lot of regulation within government to control all those elements.

Mr. Mike Allen: Maybe you can clear something up for me, because I've obviously misunderstood. You say “The second management policy instrument that we are responsible for is the Privacy Impact Assessment Policy, which was implemented in 2002.” You go on to talk about it, and the next paragraph says “We are currently reviewing this policy and we are working in close collaboration with the Office of the Privacy Commissioner on this matter.”

This is six years later, and this was actually implemented. But you say “We expect that our review will be completed within this fiscal year.” What does that mean? I've obviously misunderstood that. Why would you be reviewing that six years after it was implemented? What is that review? What is the context of it?

Mr. Ken Cochrane: This falls within the broader space of policy suite renewal. Before we began the exercise on policy suite renewal, the Government of Canada had a whole series of management policies that departments needed to follow. I believe that the number of management policies when we began the review was about 180. Our sense was that this was a very large number of rules for departments to try to follow. As we've gone in, we've tried to collapse and combine things, as much as possible, into logical chunks. We've reduced the 180 policies to about 44.

In this particular case, we had two separate policies. One was on PIAs, privacy impact assessments, and one was on privacy. We've put them together, because they logically fit together. This is not so much reassessing the privacy impact assessment itself as it is putting it in the family. As we put it under the umbrella so it's easier for departments to use, we'll work with the Privacy Commissioner to make sure the process for privacy impact assessments is most logical.

● (1615)

[*Translation*]

Le président: Mr. Crête, please.

Mr. Paul Crête (Montmagny—L'Islet—Kamouraska—Rivière-du-Loup, BQ): Good afternoon.

The Privacy Commissioner wants the authority to disclose information in the public interest on government institutions' management practices in the area of privacy. Ultimately, from what I understand, it wants to take snapshots of the efficiency of each of the organizations and make them public.

What do you think of that recommendation? Should we include it in the act?

Mr. Donald Lemieux: I wasn't here when Ms. Stoddart made that comment. I don't know under what circumstances she made it.

In fact, under the act itself and the policy, there are restrictions on departments that want to disclose... There are rules, under the policy and the act itself, for departments wishing to disclose personal information.

If I correctly understood the example she gave, this is a photograph that—

Mr. Paul Crête: I'm not talking about a photograph, but rather a snapshot of the situation, of the management by an organization. She would like us to be able to show the management practices of such and such a government institution or another in the privacy field, and for that to be included in the act so that the public can judge the efficiency of each of the organizations.

Mr. Donald Lemieux: I think I understand now.

In fact, she would like there to be greater understanding of the statistics and an annual report to Parliament. One of the things I mentioned about the Accountability Act is that the Treasury Board President was specifically mandated to gather statistics, which we were doing in any case, as part of our role.

Obviously, we haven't restricted ourselves to our discussions with the Office of the Information Commissioner; we also have discussions with the Privacy Commissioner.

Mr. Paul Crête: Do you think it would be desirable for that power to be included in the act? It isn't right now.

Mr. Donald Lemieux: For the moment, as part of our role, we're exploring the possibility of adding it to the policy and of working with the Commissioner's office to try to reinforce certain areas.

Mr. Paul Crête: In another connection, a directive on social insurance numbers covers government organizations. This week, we had quite an extravagant example: Chrysler lost a data base containing 250,000 names of individuals and their social insurance numbers. We're also surprised that the private sector has people's social insurance numbers.

Does your directive provide that every organization must protect the use of that informaion and that it may only transmit it to private sector individuals in exceptional cases or specific cases prescribed by regulation?

Mr. Donald Lemieux: That field is shared with Service Canada. We are responsible for monitoring government institutions with regard to social insurance numbers.

I would like to emphasize that a social insurance number is also a piece of personal information. However, the Privacy Act makes no mention of social insurance numbers. In 1988, I believe, we issued a policy on that matter. Social insurance numbers are such important pieces of personal information that we established a policy in an attempt to control them.

Mr. Paul Crête: Does your directive provide that the use and transmission of that information by the private sector is controlled for every organization?

Mr. Donald Lemieux: The directive itself provides that institutions must restrict that use in accordance with their mandate. Our website provides a list of statutory reasons for which social insurance numbers can be used, as well as the programs that are authorized.

● (1620)

Mr. Paul Crête: Does it mention instances in which they may be transmitted to the private sector?

Mr. Donald Lemieux: If I may supplement that, I think that will answer your question. In some cases, there may be programs or acts as a result of which there may be a sharing with other sectors. That's provided for in the agreements between the departments and—

Mr. Paul Crête: Would it be appropriate to have a similar directive for the private sector on the use of SIN numbers as a result of the excesses that have occurred in the various departments?

Mr. Donald Lemieux: In the private sector, SIN numbers are considered a piece of personal information. They should therefore be protected. Regardless of whether it's DNA or whatever, it's protected in the same way. Unfortunately, there may be cases in which personal information—SIN numbers or other items—may be disclosed. As Mr. Cochrane said, the aim is to protect them as far as possible.

[*English*]

The Chair: Thank you.

Monsieur Harvey.

[*Translation*]

Mr. Luc Harvey (Louis-Hébert, CPC): I'll continue in the same vein as Mr. Crête. If I'm not mistaken, a social insurance number is required when a cheque is issued. Yes or no?

Mr. Donald Lemieux: Yes.

Mr. Luc Harvey: So a private business winds up with a social insurance number if it issues a pay cheque to its employee. It has no other choice but to obtain its employee's social insurance number.

It's not a problem for me if the business has the SIN number. But how does it manage to let it escape? Is its ability to make money from that list of social insurance numbers regulated or limited? Are there any safeguards against that?

Mr. Donald Lemieux: I mentioned that there are agreements between the departments and the private sector. It's the same thing for the banks. At Revenue Canada, for certain provisions, the banks must have access to social insurance numbers. That's protected in the private sector by PIPEDA. Those institutions are governed by that act at the federal level. There are comparable acts in other provinces and territories, where that information is protected as personal information. On the one hand, it all makes sense.

For us, the SIN is a number that was created by the federal government. In the private sector, as a result of agreements with the departments, or programs or acts, businesses have that number. It's protected at the federal level by PIPEDA and by a provincial statute such as the Ontario—

Mr. Luc Harvey: Are there coercive ways to ensure that private businesses are prudent in the way they protect social insurance numbers or personal information that they may hold on their employees?

Mr. Donald Lemieux: Do you mean with regard to identity theft?

● (1625)

Mr. Luc Harvey: Let's suppose someone discloses a list of information including 250,000 social insurance numbers with names and a set of information. Are there any fines? Can a citizen say that you lost his personal information and that there will be costs? There's also increasing talk about identity theft. That's what I want to get to, identity theft. If we can't protect those who have information... When I buy a car, I don't have the choice of whether to say who I am in order to get the keys. I have to give my name, my address, my telephone number, my mother's name, my bank account number and my social insurance number. That's normal; a $30,000 vehicle is being entrusted to me. Once the dealer has that information, which I give it confidentially, if it isn't careful enough—

Mr. Donald Lemieux: No criminal penalties are provided for in the policies, whether it's ours or that of Service Canada.

Mr. Luc Harvey: Does a citizen have any recourse against the business?

Mr. Donald Lemieux: That's not my field, the field of the policy —

Mr. Luc Harvey: Would it be good for there to be one?

Mr. Donald Lemieux: You're talking about a theft, a crime. That's a justice matter. If someone steals an identity or does something illegal with personal information belonging to someone else, I would say that is more of a Criminal Code matter. The RCMP or the police would conduct an investigation, if there was a theft or some form of abuse. That's straying a little from my area of responsibility.

Mr. Luc Harvey: Do you feel you have the necessary tools to control identity theft? Ultimately, if you don't have enough information on an individual, you don't know whether it's him or someone else who is before you. You are entitled to some information that is relatively easy to find, but, as for the rest, you don't know whether it's really Luc Harvey who's talking to you on the telephone or who appears before you to apply for a passport. So what tools do you have, or what tools would you need to ensure that it is indeed the right individual, the one you should be dealing with, or the one who says he bears a certain name. I bear the name of Luc Harvey, and I can prove it, but someone else could come and call himself Luc Harvey as well.

Mr. Donald Lemieux: I believe Mr. Cochrane would like to add something regarding identity theft.

Mr. Ken Cochrane: May I answer in English?

Mr. Luc Harvey: Yes, there's no problem with that.

[*English*]

Mr. Ken Cochrane: In the area you're talking about, if there were to be sanctions or whatever, PIPEDA needs to deal with that with respect to private industry. As Mr. Lemieux says, it's a criminal matter when information is stolen, so we're into the criminal side of this process.

Identity is an area we're also engaged in on behalf of the Government of Canada. It's a new area. Different institutions determine the information required to verify that you are who you say you are and I am who I say I am. We're working collectively on identity standards across the country, with all the jurisdictions. We're also speaking to the banks and others about identity standards. Is my social insurance number, my driver's licence, and my passport sufficient to identify me? It's an area we're very active in right now. I don't have a solid answer. I can't tell you three things we'll accept.

It's all part of registering and establishing the person. We're a little outside of our discussion here. But registering and establishing a person is the most important part of the process. As an institution, you need to determine that you're satisfied that this is Mr. Lemieux. Once you've done that, we have tools we will put in place as part of identity management.

[*Translation*]

Mr. Luc Harvey: Should that be defined? That's my question. Do you have everything you need? We know that fingerprints are roughly 92% effective, because there are certain problems. With voice, we're getting to an effectiveness rate of roughly 30%. Retinal identification has a much higher rate, and for DNA, it's even higher.

[*English*]

Mr. Ken Cochrane: I agree. It's a leading-edge area for all of us: the Americans, the British, the banks, and everyone else. It's an area we're very active in. The possibility exists that we will put some controls in place. From a policy perspective, what that means in terms of legislation—

An hon. member: You'd be happy if she didn't.

The Chair: Mr. Hubbard had a brief item.

Hon. Charles Hubbard: Within the public service, there are tens of thousands of employees who have accessed different types of information. In your policies, how do you ensure that employees of the government do not divulge, lose, or carelessly leave information? What happens when they do? Is there a policy? I don't want a long description. Is there a policy to deal with people who handle other people's private information?

Mr. Donald Lemieux: Like so many of these things, it cuts across a bunch of areas. If you're talking about federal public servants, you already have some human resources issues if someone is mishandling information. Employees have clearances so that they can handle information at a certain level. It breaks down into Protected A, Protected B, Protected C, Secret, Top Secret, and that kind of thing. As an employee, you're limited in what you have access to. If you don't have access to that information, or you shouldn't have access and you do, then perhaps there's a sanction from a human resources perspective.

There are also various disciplinary measures. If someone has access who has committed an offence, we're looking at the Criminal Code.

● (1630)

Hon. Charles Hubbard: So you do have policies and you do have classifications and material on people with different security...?

Mr. Donald Lemieux: Absolutely. It cuts across security, privacy. If there's a breach, it's a Criminal Code offence. It could be a number of things.

Mr. Ken Cochrane: There is policy around the use of electronic networks, which really allows people to have access to systems and so on, so there are very strict policies.

Hon. Charles Hubbard: You do have strict policies.

The only other observation, Mr. Chair, would be that if we are making recommendations on this legislation, as Mr. Wallace said, we vet this back through your organization, so we don't get involved in something that is a problem for everybody.

Maybe, Mr. Chair, we'd want to take and look at it before we conclude our report and make sure Mr. Cochrane and Mr. Lemieux have at least a chance to have some input on what we suggest in terms of what we already see from the commissioner.

Thank you, Mr. Chair.

The Chair: Thank you. Good.

Mr. Wallace.

Mr. Mike Wallace: One of the recommendations—and I don't expect you to comment on the recommendation—is:

> The Act should be strengthened with respect to the provisions governing the disclosure of personal information by the Canadian government to foreign states. Treasury Board Secretariat (TBS) has taken some important steps by providing guidance on information sharing agreements and outsourcing of personal data processing.

And then she goes on to say:

> However, we need privacy protections related to cross-border information sharing enshrined into law.

Can you just tell me, in sort of a thumbnail approach, in terms of providing guidelines and information on information sharing agreements and outsourcing, what you provide departments on information that might be shared across the border now? What exists now?

Mr. Donald Lemieux: Mr. Chair, there are a couple of things I'd mention on that front.

First of all, there's the work we did at the Treasury Board Secretariat going back a couple of years now, maybe three years, on the U.S.A. Patriot Act. There had been a complaint in B.C. regarding some employees, and the federal government became engaged because we were talking about the transfer of personal information. We got involved, our division got involved—because of its policy role in terms of sharing personal information—in developing some tools, some guidelines for government institutions when it comes to contracting and sharing information. We worked very closely with the Privacy Commissioner, and we issued a report, I believe just over a year ago maybe—years seem to come and go pretty quickly here—called *Privacy Matters*, in which we gave pretty solid policy direction on what should be done.

We're also working on additional guidelines and advice on transborder data flow. We've actually shared a document with the Privacy Commissioner on issuing guidelines on that, and we're still going back and forth. It's obviously an area that's sensitive, and I think everyone's aware of that, so we're just trying to be as careful as we can.

Mr. Mike Wallace: That document was called *Policy Matters*?

Mr. Donald Lemieux: No, *Privacy Matters*.

Mr. Mike Wallace: Is that a public document? Can I get a copy of it?

Mr. Donald Lemieux: Yes, it's up on our website.

Mr. Mike Wallace: Thank you very much. Those are my questions.

Mr. Donald Lemieux: It deals with the contract provisions. It's exactly one of those tools departments find useful because it has templates, tools. If you're issuing a contract, and you're dealing with a certain level of—

Mr. Mike Wallace: It's the nuts and bolts on the how-to of these things?

Mr. Donald Lemieux: Yes, it's very much a how-to.

Mr. Ken Cochrane: If you're outsourcing something, it suggests how you need to word the contract to protect Canadian information that might be held by the outsourcer.

Mr. Donald Lemieux: It was very well received in that regard, I think.

Mr. Mike Wallace: Thank you.

The Chair: Thank you, Mr. Wallace.

Flowing from that, as you know, the committee has resources from the clerk side, the responsibilities, as well, from the Library of Parliament, and our researchers are taking command of information and trying to coordinate it for us. I guess there's a request for you, and I'm going to ask our researcher, Nancy Holmes, if she would just make a request to you to help us to the extent you are able.

Ms. Holmes.

● (1635)

Ms. Nancy Holmes (Committee Researcher): It was just following up on some questions you've already had, I think, from Mr. Hubbard and Mr. Wallace, and just sort of tightening it.

You said you haven't had much opportunity to look over the document that the Privacy Commissioner prepared, and that's sort of setting the framework for what this committee is doing in terms of its study. So it might be really helpful if the committee were able to get something back from you in response to those recommendations, particularly the recommendations dealing with putting into the act existing Treasury Board policies.

The Chair: Okay.

To the extent that you have some input that would be helpful to the committee vis-à-vis those recommendations or related to them, we would appreciate receiving that.

Finally, before we excuse you, when we started I asked the question about state of the union under the umbrella Treasury Board is responsible for. When we did the estimates for the Office of the Privacy Commissioner, one of the most significant areas of discussion, which actually has carried forward now into this, our review of the reform of the Privacy Act, had to do with the human resources situation in the Office of the Privacy Commissioner, the capacity problems, the training level problems. As well, there was an identification that the impact assessments from around the government departments and agencies weren't working, weren't helpful.

It would appear that the Office of the Privacy Commissioner has a significant human resources problem. It has a problem with staff. The turnover has been so high that the service levels have not been met. Backlogs are out of control. The act has not been looked at in 25 years. I didn't get the sense that you were concerned about this.

I'll ask you again. Given those facts, is there anything we can expect from Treasury Board to help move the attention of the public service—which tries to make all this work—to make sure that we're supported in these observations and that there is in fact a collaboration to the greatest extent possible that we're going to deal with human resources situations that are not just from the Privacy Commissioner? We heard it from the Information Commissioner as well as from other departments. Maybe we'll refer some of this to the government operations committee. The state of the union is not good, in my view, and I suspect many members would agree.

I'm not going to put you on the spot to answer right now, but I can tell you we have a responsibility to report on this, and I think it's going to take some time. Now we're faced with, as you know, in these ten recommendations and whatever else may come up, moves or interest levels or developments within the privacy regimes across the country and internationally to expand the level of activity and the responsibilities of privacy commissioners, which is going to require even more human resources. I don't know where it's going to come from, but the system we have right now can't even keep up with the responsibilities the Privacy Act already requires of them.

So I think we have a serious problem here. I want you to know that this seems to be a preliminary assessment. But if you have some input on that as well, I would ask you—not now—to provide us with some feedback on your assessment of the state of the union of the Privacy Commissioner vis-à-vis the areas of responsibility the Treasury Board Secretariat has. You laid them out in your speech: sound management practices for the handling and protection of personal information; clear decision-making and operational responsibilities are assigned within government institutions; consistent public reporting. This does not appear to be happening, and it's important.

I think we're going to leave it with you that there are some concerns. You may be able to give us some assurances of how this is being addressed—or will it be addressed? How could it be addressed, and how could we as a committee participate in supporting initiatives to make sure that the fundamental operational problems that we're apparently seeing are going to be addressed in a responsible fashion?

Is that fairly clear?

● (1640)

Mr. Ken Cochrane: That's fair.

I just want to comment on one aspect of it. We do work very closely with both commissioners for the very reason that we want to make sure that the legislation or the policy is well implemented in departments. And on a few things you made note of—I think on the privacy impact assessment—we know there's a horrendous backlog with the Privacy Commissioner. These are areas where, regardless of funding, we're trying to work together to break that backlog by doing things differently.

I think your resources are always a factor for all of us, but we have to look at ways to be more efficient. So there are ideas we've worked on together to try to reduce the load that arrives at their door. We'll play a different role; we'll put more responsibility on departments. I think there's a balance between adding resources and trying to improve the flow of information and to change the process and simplify it for departments and to simplify it for us and the commissioners. This would be true with both commissioners.

The Chair: Okay. The committee would appreciate your input to the extent that you think it would be helpful to the committee. I'll leave it with you to decide.

Thank you, Mr. Cochrane and Mr. Lemieux, for attending. You're excused at this time.

We have a little bit of business before we adjourn.

On witnesses, I just want to advise members so that they can be apprised. The clerk can give you a little projection.

The Clerk of the Committee (Mr. Richard Rumas): Thank you, Mr. Chair.

The next committee meeting will be Tuesday, May 6, when we have the Canadian Internet Policy and Public Interest Clinic. They will be accompanied—we're waiting for final confirmation that this is going to happen—by the Canada Border Services Agency.

Next Thursday, May 8, we have a man who wore many hats, including the first Privacy and Information Commissioner of British Columbia, Mr. David Flaherty.

The following Monday, which is the 13th, we have asked for the RCMP, CSIS, and the CSE.

On the 15th, which is the Thursday, we have Mr. Paul Comeau and Professor Michael Geist, who are, as you may have seen, on the Office of the Privacy Commissioner's advisory panel on reform of the Privacy Act.

Then there is a break in May. After the break, we have scheduled for May 27, which is a Tuesday, the minister with his officials from the Department of Justice. We're still working on the 29th, and tentatively we have scheduled the Canadian Bar Association for June 3. That Thursday may be the last sitting of the committee if the House follows the parliamentary calendar.

So that's where we are right now, Mr. Chair.

The Chair: And there are also one or two provinces—I believe New Brunswick and Nova Scotia—that have recently completed reviews, so they're very fresh on things. We may be having one or both of those before us.

That's just to give you a heads-up. This will be given to you in writing, but I wanted you to know that we have made some progress on that.

Mr. Wallace, you had something.

Mr. Mike Wallace: Just for the clerk, our House leader loves to remind us that the House actually sits until June 20, not June 6. Those shaded areas are just in case there is an extension.

I appreciate that you've done a lot of work in getting people here, and I think we have lots of time during the last couple of weeks.

The Chair: We have time. Doing a report will also take—

Mr. Mike Wallace: I wanted to make sure they didn't not show up after that because they saw the orange on the calendar.

The Chair: I think it will be appropriate for us also to have the Privacy Commissioner herself come back to wrap this up and give us a little time. But we are doing a little work. As you know, our support people from the Library of Parliament do a lot of work as we move along.

Are there any further comments from the committee?

The meeting is adjourned.

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
