House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 003 • 1st SESSION • 39th PARLIAMENT

EVIDENCE

Monday, June 5, 2006

Chair

Mr. Tom Wappel

Standing Committee on Access to Information, Privacy and Ethics

Monday, June 5, 2006

● (1530)

[*English*]

The Chair (Mr. Tom Wappel (Scarborough Southwest, Lib.)): We're going to get started. Committee members, just so you're aware, we only have 89 minutes. We have to adjourn at 5 o'clock on the nose because the Bill C-2 committee is starting its deliberations at 5 p.m.

On that note, there is a very good likelihood that we will not meet next Monday because the Bill C-2 committee doesn't look like it's going to be able to complete its work by the end of this week. Therefore, it's very likely that it will continue on Monday, and as we know, if they're working we can't. So we'll keep you informed of that. If something happens, the Information Commissioner is scheduled to appear, as he was today, and the Registrar of Lobbyists.

So without further ado—

[*Translation*]

Yes, Ms. Lavallée.

Mrs. Carole Lavallée (Saint-Bruno—Saint-Hubert, BQ): Exactly how much time do we have?

The Chair: We have 88 minutes.

Mrs. Carole Lavallée: That gives us a grand total of 158 minutes since the beginning of May. Thank you, Mr. Chairman.

[*English*]

The Chair: I don't want to hold up while waiting for electronic means. The Privacy Commissioner has been kind enough to provide us with a paper copy of the documents, so allow me to introduce our witnesses and let them get right to their presentation.

First, of course, we have Jennifer Stoddart, the Privacy Commissioner. Welcome. And we have Heather H. Black, assistant commissioner, PIPEDA, the Personal Information Protection and Electronic Documents Act.

Parenthetically, members, the five-year mandatory review, for reasons best known to others, was referred to the industry committee. I and the chairman of the industry committee, Mr. Rajotte, have written to the House leaders, with the support of Mr. Tilson, to suggest that the reference should be to this committee. We haven't heard back yet from the House leaders, but hopefully the logic of that will dawn on them and they will refer that act to us.

And we have Raymond D'Aoust, assistant privacy commissioner.

Welcome to all of our witnesses. We'll start with Ms. Stoddart, who has a presentation, as you can see before you.

You have up to 20 minutes, but in view of the length of time we have and the questions that no doubt will come, we'll ask Ms. Stoddart to keep it in the vicinity of 15 minutes.

Ms. Jennifer Stoddart (Privacy Commissioner, Office of the Privacy Commissioner of Canada): Good afternoon, everyone.

● (1535)

The Chair: No matter how fast computers are, they're always slow when you're waiting for them.

Ms. Jennifer Stoddart: Thank you very much, Mr. Chairman and honourable members, for inviting me here.

On the screen you will see an overview of the presentation that I hope to run in the next 15 minutes, which I hope will give you an initial introduction to our role and mandate, the laws we administer, and some of the key issues.

[*Translation*]

I'll begin by explaining the role and mandate of the Office of the Privacy Commissioner. Unlike other provincial offices, the OPC is an ombudsman office with several roles, the most important of which, from a resources standpoint, is to conduct investigations.

The OPC also conduct audits under two federal privacy laws. Furthermore, it publishes information about personal information-handling practices in the private sector and brings privacy issues to the attention of Parliament.

Although it requires minimal resources, public education is one of the OPC's most important roles, as is research and policy on emerging privacy issues.

[*English*]

We administer two laws, and you're going to hear a lot about the first one in the coming weeks. This is our basic federal government Privacy Act. It came into force about 25 years ago, and this is your basic set of ground rules for the public sector. It's standard in terms of international data protection. Standards now are fairly low. You can use information collected from the public as long as it's directly related to a program or to an activity. You don't need the consent of Canadian citizens, and you don't need to inform them in any direct way about how you're using their information.

Since 2001, the second law we've been administering is our newest privacy law in Canada known by its acronym, PIPEDA, but you can call it the PIPED Act or...there are various ways of pronouncing it. It is now fully in force and it applies to the jurisdiction where the federal government has authority—-federal works and undertakings, federal crown corporations that might have private-sector-related activities, and activities of trade and commerce in Canada under section 91 of the BNA Act. Like its counterpart, it sets out rules. These consent-based rules are far more extensive and the standard for privacy protection is a lot higher.

In the last few years, one of the important goals of the office has been to work cooperatively with the provinces and the territories. Some of you will know that privacy protection is also a provincial jurisdiction because provinces have authority over property and civil rights. Privacy is a civil right. It's a human right in the Canadian context, so it was important for us at the Office of the Privacy Commissioner to work cooperatively with the provinces to make sure Canadians have seamless privacy protection as much as possible. I can give you some examples of various joint efforts with the provinces.

Very briefly, some of our current key issues and concerns are these. Under the Privacy Act, the national security agenda, we appeared on the Anti-terrorism Act last spring. We have been asking questions about the purview or the extent to which the Anti-terrorism Act has reduced the individual right to privacy under the Privacy Act as it is now constituted. We're concerned there's less reason for judicial authorization. We think the judiciary is key, that the judicial authority be there when you're going to regiment individual rights and liberties. And we're giving Canadians less opportunity to challenge the curtailment of their freedoms.

On a separate issue, we're also concerned about the increasing blurring of the lines between the private sector and the public sector. In Canada, we're used to the state carrying out laws, certainly carrying out criminal law and national security issues. With a change to PIPEDA that came about two years ago, organizations in Canada are now mandated to specifically request information, to collect it for the express purpose of giving it to the national security authority. Again, this is a trend we want to watch.

The transborder flow of information has been a constant theme in the last few years. There are two major subsets of issues. The first issue is what happens to our information at the border, information we are specifically sharing at our land and air borders, particularly our land border with the United States, given the flow of people and traffic to the United States. We have just finished a first audit of the handling of personal information at some of the land crossings by the Canada Border Services Agency, and we'll be publishing that in our next annual report on the Privacy Act that will come out at the end of June.

● (1540)

We also just received the draft rules for the do-not-fly list from the Department of Transport. We'll be doing a privacy impact assessment on the ground rules for the do-not-fly list.

The second set of issues is known now as the issues linked to the U.S.A. Patriot Act. They're not a U.S.A. Patriot Act set of issues per se; they are issues of transborder data flow—the global flow of our personal information. It has become accentuated in the last few years. It has existed for decades now, but what happens to Canadians' personal information once it leaves the borders of Canada and Canadian law has just recently come to public attention.

The Chair: Madam Stoddart, can I stop you for just one second? I want to inform the committee that those bells are not an annoying signal; they actually mean something. There is a vote. The vote will take place in about 22 minutes—something like that.

I suggest we let Madam Stoddart finish, and then we can decide that either we're all going to stay or we'll all go to the vote. Then we'll come back, assuming there's at least half an hour left. I don't know what the vote is about or how long it will take—oh, it's to proceed to orders of the day, so some games are being played, I gather.

I don't think it's fair to have the witnesses stay here and wait if none of us returns. If we can get back here by 4:30 p.m., then at least we'd have another half-hour before we'd have to adjourn.

Without further ado, let's allow the Privacy Commissioner to finish her comments.

Ms. Jennifer Stoddart: Well, thank you. I'll try to be economical.

One of the requests of this committee as it was constituted in the previous Parliament was that we table a paper on Privacy Act reform. This was the first law. The law is now 25 years old, and I've consistently been criticizing it for its inadequate protection of Canadians' personal information.

At your request, Mr. Chairman, I have formally tabled with you our first paper on Privacy Act reform. Some of the issues have to do with transparency. We talk about transparency and accountability; we're saying the government should be accountable not only for amounts of money, for projects, but should also be accountable for Canadians' personal information.

Canadians should have a right to see what's in their files now, but they virtually have no further rights. They cannot request in front of a court that this information be corrected if it's erroneous. Lord knows, sometimes we all have mistakes in our government files; you have no right of correction if the government does not want to correct it. You have no right of damages, as was recently confirmed by the Federal Court in the Murdoch case.

It is virtually impossible for Canadians to track where their personal information is going now. As blood flows through arteries, it takes experts, and even then.... There's a publication called *InfoSource*, but *InfoSource* is out of date and it's often erroneous.

Basically what we're saying, Mr. Chairman, is that the federal government should live by the standards it's imposing on the private sector—ask for the same transparency, accountability, and privacy policies it now asks of companies under PIPEDA.

Apart from the basic reform of the Privacy Act, in the meantime, because this is not perhaps a simple affair....

● (1545)

[*Translation*]

One of the current key issues is ID management. The call to identify the individual in each transaction and to have a secure, reliable identity that cannot easily be stolen is becoming increasingly prevalent. At the same time, however, measures must not represent an unwarranted invasion of privacy. Nor should there be too many demands made in terms of sharing information with the government or a financial institution. These are just a few of the ways in which identity is used.

Another key concern of ours is surveillance. Recently, we have put particular emphasis on video surveillance. Guidelines have been published on our website. Video-surveillance, which is prevalent just about everywhere in the workplace and on the streets across Canada, falls under both federal and provincial jurisdiction and affects each and every one of us. In Toronto, for example, consideration is being given to installing video-surveillance devices on buses and in the subway system. Other municipalities will likely soon follow suit.

The OPC has reached several conclusions as to the legality of video-surveillance in the workplace, pursuant to private sector legislation. Generally speaking, the direction advocated by the OPC has the backing of the Federal Court.

[*English*]

The third key issue that I bring to your attention is the whole burgeoning issue of health information in Canada. Again, like so many of these issues, it's provincial jurisdiction and also federal jurisdiction, because all this information crosses provincial boundaries. As well, the federal government has its own employees, the veterans hospitals, and so on.

When PIPEDA came into force we worked very closely with health providers, notably the Canadian Medical Association, and developed some 75 frequently asked questions about health information on the website.

The fact that the whole health sector was legislated was a bit of a shock back in 2002-03. I think things have calmed down, and the whole health sector is now used to the idea of having a program for the management of personal information. Ontario has moved to adopt its own health information act, and Quebec has had one for many years. So it's an area where we're working with the provinces.

One of the issues we're monitoring is the unfolding of electronic health records across Canada, notably through Canada Health Infoway. It has a billion-dollar budget to assist with the development of electronic health records. In order to make sure that the framework for the management of electronic health information respects privacy principles, we're working with Canada Health Infoway and the provinces. Those are some of the issues in the public sector.

In the private sector, I'll quickly go to anti-spam issues and the need for strong anti-spam legislation. This is something that preoccupies not only the Office of the Privacy Commissioner but the police, because of what spam now carries. It's not just an annoyance or a giggle, depending on what's in the spam message. It carries serious viruses and spyware, and it is a threat to critical infrastructure security as well. This is an issue of competition and consumer protection, and any spam legislation that comes down would probably give various agencies a different role in enforcing spam threats.

Technology generally is a concern, and you may have heard about our annual report on PIPEDA that we launched just last week. We brought to the public's attention the issue of RFIDs, radio frequency identification chips, that are being rolled out across Canada. At the moment they're only in supply chains, but soon they will be brought down to the consumer level, as they are in Europe. We have done a fact sheet with basic information on this, and we will be developing guidelines for industry and consumers in the next months in cooperation with the provinces, because of their role in regulating privacy.

RFIDs is basically a technology that's been around since Word War II, but now it's being adapted to the consumer and supply-chain-level management. I'm not a techie, but I've been told it consists of an antennae, a computer chip, and a casing. It allows this little device to emit a unique signal so that each object is uniquely identified in the universe. That means we can track objects, which is useful in the supply chain for inventory management, national security threats, theft, transportation across continents, and so on. Eventually, because we are linked to the objects we purchase or use, it will allow for the unprecedented tracking of people. They will be entered into a database by linking them with the objects they manipulate or purchase. Therefore there are privacy preoccupations.

To conclude, as an agent of Parliament we can give you policy advice, expert advice, and slants and ideas on some of the legislation that doesn't seem to have privacy implications but may. Of course, we can make appearances, at your request or our request, at various committees.

What will be on in the future? You have our reform proposal with you, and we hope you will invite us back to talk in detail about it. Many months of preparation have gone into our proposal.

● (1550)

We will be bringing out our Privacy Act report in three weeks, and in the fall there will be the review of PIPEDA. We'll see which committee we'll be called to appear before.

The Chair: Thank you very much.

I see people getting ready to go, so we'll go for the vote. The committee stands adjourned until the vote is over, hopefully no later than 4:30, so we will have about half an hour for questions.

We only need three people here to have a fully constituted meeting. I'll be one of them, so if two people can come back, we can at least get some questions in.

● (1550)

(Pause)

● (1635)

The Chair: We have 24 minutes, and that doesn't give us enough time to do our normal rounds, so it's been suggested by the clerk and members of the committee that we have one question per party, starting with the official opposition, and just keep going until we run out of time. Does that meet with everybody's approval? If somebody doesn't have a question on the first round, they can always jump in on the second round. I don't hear any “nays”, so that's how we'll proceed.

Would anyone on the Liberal side like to go?

Mr. Regan.

Hon. Geoff Regan (Halifax West, Lib.): Yes, Mr. Chairman, I'd be happy to do that as soon as I find the note I'm looking for. There are a couple of things, actually.

You were talking about the RFIDs, and I guess I'd like to know what your view is. I read about this on the weekend. Companies are claiming that they would only use the RFIDs on pallets—you know, the larger cases that contain smaller boxes—and not on individual boxes that are sold to consumers. I presume you don't see a particular problem with that as long as the RFID doesn't go with the consumer out the door as part of the item they've bought. Is that a fair question?

I shouldn't use that as my only question, mind you, so I'll add to that.

Ms. Jennifer Stoddart: The answer is yes.

Hon. Geoff Regan: In terms of the concerns you expressed about privacy matters, have you examined the proposed accountability bill in relation to access to information matters and matters related to privacy, and what are your thoughts on it?

Ms. Jennifer Stoddart: Thank you, honourable member.

I'd direct you to our latest annual report on RFIDs. Of the companies we surveyed, two indicated already that they've linked goods to personal information and one was using RFIDs to track employees. So it's moving down.

On the accountability bill, we appeared in Parliament last week to point out, notably, that we're concerned that, as it is now presented, this bill will lower the level of personal information protection in three organizations: Atomic Energy of Canada, the CBC, and VIA Rail. All are now covered by PIPEDA, as I said very rapidly. PIPEDA has a better level of personal information protection than the Privacy Act does.

To give you an example, honourable member, if you travel with VIA Rail, under the Privacy Act you have a right to see your file, and you can ask for a correction. But if they don't make the correction and you think you're right, or if there's a slip and somehow your travel information is spilled—published—and it causes you some damage, you have no right of redress. So as we pointed out, why would we take a step backwards? Personal information also needs accountability at the highest level for the Canadian public.

[*Translation*]

The Chair: *Merci.*

Do you have any questions, Mr. Laforest?

Mr. Jean-Yves Laforest (Saint-Maurice—Champlain, BQ): Good day, Ms. Stoddart.

You stated in your opening remarks that one of the OPC's important roles was to educate the public about the measures employed to protect identify theft. This is one of your Office's responsibilities.

Do you have an overall plan of action to educate the public about this issue? Have you planned for follow-up action? Do you have an idea of the results? Is the general public aware that right now, a number of organizations have important personal information about them on file in their data banks?

● (1640)

Ms. Jennifer Stoddart: Mr. Chairman, if I may, I'd like to ask Deputy Commissioner Raymond D'Aoust who is responsible for this particular area to answer Mr. Laforest's question.

Mr. Raymond D'Aoust (Assistant Privacy Commissioner, Office of the Privacy Commissioner of Canada): Yes, sir, we do have a communications and public education plan in place. One of our branches is dedicated entirely to this effort.

To further our understanding of this subject, we commissioned several public opinion polls, one of which will be made public shortly. The findings show that the Canadian public do not have a very clear understanding of privacy and of various related legislative provisions.

We know that the need is great. We have focussed our efforts on small and medium-sized enterprises. Working with an expert-adviser on the subject, we are developing an on-line training module. We hope to develop tools of this nature to help SMEs comply with the legislation.

[*English*]

The Chair: Mr. Wallace.

Mr. Mike Wallace (Burlington, CPC): Thank you, Mr. Chairman. I'm new here, and this is all new to me, so these are probably fairly elementary questions. In your report, you talk about there being similar legislation in the provinces. Are there any major gaps between our legislation and the provinces', and could you explain what they are and the significance of those gaps?

Ms. Jennifer Stoddart: There's a very complex picture. Maybe I'll start the answer and the assistant commissioner, Heather Black, could complete it, as she was a long-time general counsel and knows....

This is an area of joint jurisdiction, and only three provinces have chosen to go ahead in this area with legislation of their own that meets the test set up in PIPEDA of being substantially similar. I'm sorry, it's three and a half, I guess, if you count health in Ontario.

This law is set up such that the federal legislation applies to the federal sector and commercial activities, unless the province has its own legislation. Quebec has had private sector legislation since 1995. Then Alberta and B.C. have had their own legislation since 2003, and Ontario since 2005.

Do you want to add to that?

Ms. Heather Black (Assistant Commissioner (PIPEDA), Office of the Privacy Commissioner of Canada): There are significant gaps. For example, in the province of Manitoba, where there is no substantially similar law and PIPEDA applies, it applies only to commercial activities. It covers the federally regulated private sector for customer information and employee information. When you move into the provincially regulated private sector—say the retail level, or what have you—it only applies to customer information, so for all of the employees of those organization there is no protection.

The other gap is in areas where the federal law simply cannot go; that is, such areas as health, education, municipalities, schools, hospitals—all of that. That's an enormous gap.

Mr. Mike Wallace: Are there ongoing conversations to try to improve in those gap areas, or is it an issue that's on the back burner for the provinces?

Ms. Heather Black: It appears to be on the back burner for the provinces. The only way those gaps can be closed is if the provinces act, because the federal Parliament cannot.

The Chair: Just so I understand it, we're talking about only PIPEDA here, or PIPEDA-type acts, not privacy. Do all of the provinces have their own privacy acts?

Ms. Heather Black: Yes.

The Chair: Are they more or less the same as the federal acts?

Ms. Heather Black: Pretty well.

The Chair: All right. Thank you.

Mr. Dhaliwal.

Mr. Sukh Dhaliwal (Newton—North Delta, Lib.): Thanks, Mr. Chair.

My question, through the chair, is about the Access to Information Act. You said you had some suggestions and that there are some gaps and loopholes. Are they department-driven or are they politically motivated?

● (1645)

The Chair: Mr. Dhaliwal, I'm sorry, what were you referring to?

Mr. Sukh Dhaliwal: The gaps. Madam said the information act we brought in does not meet the highest standards of accountability. If we say it does not meet the highest standards of accountability, where is it lacking? Are those lacks department-motivated, or are they politically motivated on the government's side?

Ms. Jennifer Stoddart: I'd say, honourable member, that they are perhaps technically motivated. The Privacy Act was brought down as a companion piece of legislation to the Access to Information Act. The other honourable member was talking about the provinces. Most provinces regulate these together.

The federal government has chosen to regulate privacy and access in two acts, with two commissioners. When the drafters of legislation change something in the Access to Information Act, they're used to making mirror changes in the Privacy Act. Something like this seems to have happened with the new legislation. That was the answer we got: it's a matter of symmetry between the two acts. Therefore, it's a drafting issue. But I would submit that we have the drafting skills to be able to say that even though these organizations would be subject to access to information under the federal Access to Information Act, we could find a way nonetheless to make them still subject to PIPEDA for the protection of personal information.

I don't know whether that's clear. Usually if you're subject to the Access to Information Act, you're subject to the Privacy Act—not always, but with a very few exceptions. So it's that kind of issue, but I don't think it's surmountable, and I do think it's unacceptable, for example, that in these major corporations—CBC—we would lower the level of privacy protection for Canadians and for the employees who work in those organizations.

Hon. Geoff Regan: I have point of clarification, Mr. Chairman.

You said that you didn't think the problem was surmountable. Do you mean it was not insurmountable?

Ms. Jennifer Stoddart: It was not insurmountable. I'm sorry if I misspoke.

I am sure there is a solution. It may be a little more difficult to draft, but I think it can be done.

The Chair: Thank you.

Madam Lavallée.

[*Translation*]

Mrs. Carole Lavallée: Mr. Laforest can have my time.

The Chair: Mr. Laforest.

Mr. Jean-Yves Laforest: My question ties in with one that I asked earlier. As you know, more and more people are using cell phones. For many, cell phones are their principal telephone, even at home.

When it comes to privacy over the airwaves, do you feel people are adequately informed of the potential risks associated with the use of cell phones? Does this fall within your area of responsibility? If not, shouldn't there be a law on the books requiring companies to inform their future clients of the privacy risks associated with the use of cell phones?

Ms. Jennifer Stoddart: You're right. I believe the public needs to be informed of the risks in terms of protection of personal information, not only when it comes to cell phone use. In the past, people were afraid that someone could be eavesdropping on their conversations. With the advent of technology, the problem has grown far more serious. For instance, it's possible to obtain the telephone records associated with all types of telephones, residential as well as cellular.

You've raised an important question, one that involves various technologies. Consider, for example, GPS systems that are now installed in automobiles. Do people realize that their every movement can be tracked with these systems? I mentioned radio transmitters. We're wondering if all of these products should come with a mandatory label advising users to be cautious if they have a GPS system. People can even take pictures with their telephones. Perhaps users of such phones should be cautioned to proceed carefully because their privacy could be violated.

It's an ongoing challenge and that's why increasingly we're investing in our website. In our view, it's the best interactive way of reaching Canadians. Our website contains a great deal of information about new technologies and we encourage people to check it out.

● (1650)

Mr. Jean-Yves Laforest: Are there provisions in place that currently require companies to disclose the potential risks associated with the use of this technology?

Ms. Jennifer Stoddart: No. As mentioned, PIPEDA spells out the requirement to educate the public about the overall information management policy. And that's what we do in terms of personal information, access to a person's file, etc. However, I don't think this legislation can be interpreted as requiring a warning of some kind, particularly on new technology products, about the possibly privacy implications associated with the use of the product.

Mr. Jean-Yves Laforest: Don't you think it would be interesting to explore this matter further?

Ms. Jennifer Stoddart: I do. We are giving the matter some thought. For example, software should come with a warning label cautioning that product use could have privacy implications.

[*English*]

The Chair: Merci.

Mr. Stanton.

Mr. Bruce Stanton (Simcoe North, CPC): Thank you, Mr. Chair.

I have a question for the commissioner.

By the way, thank you for joining us here today and putting up with a rather awkward interruption. I appreciate that.

Ms. Jennifer Stoddart: You're very welcome.

Mr. Bruce Stanton: When looking at the briefing in preparation for today, I noticed that when you have brought deputations to the committee in the past, there's been a realization that the volume of work you've had to undertake, particularly as it relates to PIPEDA, has been beyond the fiscal ability that you have to operate. I recall that progress was being made in terms of an administrative merger of the two offices of information and privacy. Is that correct?

Ms. Jennifer Stoddart: We are part of the same administrative unit for reporting purposes and formally for administrative purposes. There was a proposal that was examined by the Honourable Mr. Gérard La Forest, who's a retired Supreme Court judge and one of the primary legal theoreticians of privacy rights in his judgments. He made a study of both our offices and concluded that it would not be a good idea. His report came out in November and is on our website.

So the government has gone ahead, and then funded us separately for the future, and has looked at our funding proposals. An all-party parliamentary committee reviewed our funding proposals last November, just at the end of the last Parliament, as separate entities.

Mr. Bruce Stanton: Okay. The only comment I would offer is I certainly don't disagree with that because I would have to believe, even looking at the culture of the two offices, there are two real polarities here, and that makes a lot of sense.

Going back to the volume of work that you've got, and again in previous reports there was an indication that you did in fact have a backlog, where do we stand now, as we sit here in early 2006? Has that been brought into line now or is it at a level that is reasonable, given what you've got in front of you?

Ms. Jennifer Stoddart: No, it's not. As I explained to the all-party parliamentary committee, we think it'll take us two years to absorb the backlog, so, unfortunately, I have to report to you today that two months into the new fiscal year the backlogs are still there.

We're not pleased with the time it takes to treat Canadians' privacy complaints. We do have resources to hire new people. Our practical problem is that there is a dearth of qualified personnel in Ottawa in the civil service to fill these jobs, and as soon as we recruit people they receive other offers. I think the Information Commissioner has talked about that. So I have barely two people more than I had at the end of March, although I have all kinds of budgets and all kinds of staffing actions. So it's a real challenge. But we have two years. We're not giving up at this point.

Mr. Bruce Stanton: And as we heard your report here today, there's still a whole series of other issues in front of you, not even including the fact that you've got this backlog to deal with. So I think these are very definite issues that will need to be addressed, and we'll be interested.

I presume at some point, Mr. Chair, through the course of the coming year, we'll be reviewing estimates and/or numbers, as it relates to their budgetary requirements for the coming year.

● (1655)

Ms. Jennifer Stoddart: Yes.

The Chair: Yes, that's correct.

Mr. Bruce Stanton: Thank you, Mr. Chair.

Ms. Jennifer Stoddart: Yes, and we'd be happy to appear and discuss. We have two annual reports under both laws. We'd be very happy to go over those annual reports with you and answer your questions on those.

The Chair: Thank you.

With the committee's permission—and I hope I have it—I'd like to ask two questions in the remaining three minutes.

In your slide projection, or whatever these things are called, under the Privacy Act, you indicated that the Privacy Act came into force in July 1983, and you gave us this document, "Government Accountability for Personal Information: Reforming the *Privacy Act*". It's a lengthy executive summary, which I haven't had an opportunity to read, but I note that you say:

> To be effective, policy cannot be developed in a legal vacuum. The feebleness of the current legislation has created such a vacuum and the Privacy Act must be reformed to close the gap.

I want to give you a minute to expand on your call for a review of the Privacy Act. My specific question is, in your discussions with the bureaucracy—let's put it that way—where does the bureaucracy see a review of the Privacy Act in terms of its priorities?

Ms. Jennifer Stoddart: I'll begin. I'll ask the assistant commissioner who's in charge of that in particular to answer that.

I think this paragraph refers to the fact that we think that Privacy Act reform involves public consultation, sector-wide consultation, because this is the basic personal info management framework of all the information Canadians give to the federal government.

We think it's long overdue for reform, to address some of the challenges that I suggested: the management of personal information within the Canadian government; the management of the information that, once we've given it to the government, the government then sends abroad to our neighbour to the south, for example; to give Canadians effective rights of redress; and to do things like address issues that were largely unheard of in 1983, such as covering DNA samples.

The act deals with a definition that was quite avant-garde at the time; it deals with recorded information. Well, if you keep a skin sample, it's not really recorded information; it's just a skin sample. But we have been saying this should be treated as if it's subject to the Privacy Act.

These are some of the examples of issues. Other issues have to do with the fact that we live in such a globalized, interconnected world, and unlike for PIPEDA, we restrict the rights that people have under the Privacy Act to people who basically have immigrant status in Canada. So visitors or people who are flying through Canada on their way somewhere else, then, don't have rights under the Privacy Act. Again, there's been an administrative arrangement to get around this so that Europeans can fly in and through and enjoy the reciprocal or same level of privacy protection.

Maybe I could ask the assistant commissioner...another big thing is the whole theme of data matching.

The Chair: Assistant Commissioner, you'll have the last word. Could you just answer my question at least about where the reform of the Privacy Act is on the radar screen of the bureaucracy, never mind the government?

Mr. Raymond D'Aoust: To be honest, it's very difficult for us to come up with an assessment of that, because when we talk to our colleagues at Treasury Board, they're quite open to making any policy change that will reinforce the privacy management framework, but when we talk about Privacy Act reform, they'll say, "This is really a question for the legislator." So it's very hard.

We certainly have met with the Minister of Justice. We've met with the President of the Treasury Board. Certainly, walking out of those meetings, we felt that they were quite open to discussing Privacy Act reform.

I should say that within the parameters of the existing law, we've had some success. For instance, the Treasury Board released guidelines on outsourcing for federal managers and so on. That's done under the current legislative framework, and those guidelines, we feel, are quite good, and they're a step in the right way in terms of reinforcing or mitigating against privacy risks resulting from outsourcing.

It's the same with the privacy impact assessment policy, which was adopted by the government back in 2002. Again, we see that there's a real commitment to improving privacy management practices, but also there's a recognition that the Privacy Act needs to be overhauled, if you will.

● (1700)

The Chair: Okay, thank you.

I'm very regretful that we don't have more time, but the rules require that I cannot go beyond 5 o'clock so that there's no conflict between the two committees.

There are new members on this committee, myself included. These are very interesting issues. You've certainly given us something to think about in terms of a review of the Privacy Act by this committee. That's where the public consultation would begin, at least from the political point of view. So we want to thank you very much for that. I have no doubt that you'll be back, hopefully, once Bill C-2 is done and we can get down to some regular meetings. So thank you so much for coming.

We're 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
