House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 004 • 1st SESSION • 38th PARLIAMENT

EVIDENCE

Wednesday, November 17, 2004

Chair

Mr. David Chatters

Standing Committee on Access to Information, Privacy and Ethics

Wednesday, November 17, 2004

● (1535)

[*English*]

The Chair (Mr. David Chatters (Battle River, CPC)): I call the meeting to order.

Pursuant to the order of the House of Friday, October 8, 2004, we are considering main estimates 2004-05, vote 45, Office of the Privacy Commissioner of Canada, under Justice. The committee will also study the annual report of the Privacy Commissioner for 2003-04. The first order of business on our agenda is the call for vote 45.

With us today is Jennifer Stoddart, Privacy Commissioner of Canada, and Raymond D'Aoust.

Welcome to the committee. Perhaps you would start off with an approximately ten-minute presentation, and then we'll go to questions.

Ms. Jennifer Stoddart (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Thank you very much, Mr. Chair, for inviting us here to this new committee, which of course is very important to us since you are focused on privacy, among other things.

You've already introduced my colleague, assistant commissioner Raymond D'Aoust, who is responsible for the application of the Privacy Act. Unfortunately, assistant commissioner Heather Black, the commissioner for PIPEDA, the Personal Information Protection and Electronic Documents Act, isn't here today.

There are several officials from my office with me today, in case any of the members should have detailed questions; we'd like to be able to reply as completely as possible.

I very much look forward to working with this new committee in the months and years ahead. I'll start today with our annual report.

As you know, I was appointed Privacy Commissioner on December 1, almost a year ago. This annual report that you've just received reflects the work of both interim commissioner Robert Marleau, in helping to move the office through a difficult and complex period, and the continued efforts of the office under my leadership in the last few months, to strengthen our management and financial processes.

When I arrived at the Office of the Privacy Commissioner, I set a clear goal of rebuilding the trust of parliamentarians and Canadians in our office. I identified some key objectives; notably, to lead the office's institutional renewal in the areas of human resources, planning, budgeting, and reporting. This renewal is the critical factor, I think, in our effectiveness and efficiency as an ombudsman dedicated to the protection of privacy rights.

I also set out to help organizations fully implement PIPEDA and understand their obligations, and citizens their rights, under this new law. This involves working out shared responsibility with provinces that may already have adopted, or that will adopt, their own provincial privacy legislation.

As an ombudsman, I have a responsibility to draw Parliament's attention to the privacy implications of government and private sector activities and proposals, and to inform Canadians of their privacy rights on such issues as the growth of data banks and the introduction of privacy invasive technologies—radio frequency identification devices, known as RFIDs, black boxes, spyware, and so on. Canadians, as you know, are raising issues related to the border and international security that is posing unprecedented challenges to existing Canadian privacy legislation.

Much of the anti-terrorism legislation passed in Canada and abroad is based on the premise that the more information governments have about everyone, the safer we will be. We appeared before the House last week in that context.

[*Translation*]

Our Office is not opposed to improving security or to the sharing of necessary information among agencies. We do however raise concerns about how this is done and recommend clear procedures and policies to protect personal information, to ensure this information is not used or disclosed for purposes other than for which it was intended and not retained for periods longer than necessary.

The increasing involvement of the private sector in national security measures is also of concern and raises some important questions about the transfer of personal information about Canadians across borders. Canadians expect that governments and the private sector will collaborate to protect against mismanagement of personal information.

Informing parliamentarians and Canadians of privacy issues stems from our continued efforts to monitor compliance with the two federal privacy laws and investigation of complaints from citizens into potential privacy violations. We are also developing the Office's research capabilities to monitor new technological advances to provide timely and knowledgeable advice on the impact of legislative and regulatory initiatives and apprise the public of privacy risks.

I'd like to say a little about our efforts to rebuild the Office of the Privacy Commissioner. This has been our essential priority, as I said at the start of my remarks. Audits of the Auditor General and the Public Service Commission identified a number of serious organizational challenges in this office which I have committed myself to resolve.

I can confidently report we have made significant progress to address and remedy many of the issues highlighted in the audits. A series of corrective measures have been taken.

In particular they include implementing and strengthening our financial delegation and controls in October 2003. The Auditor General of Canada recently completed an audit of the Financial Statements of the Office and confirmed "...in all significant respects, that transactions have been in accordance with the Financial Administration Act and regulations and the Privacy Act."

We have also instituted a strategy for recovering public funds and assets that may have wrongly been appropriated. I reported on this to Parliament in April.

We've also developed a learning strategy to support executive leadership, staff training and organizational learning.

In addition, we've also created an independent external advisory board to address governance challenges, and provide advice on strategy and vision.

Lastly, we've addressed many staffing, classification and compensation/remuneration irregularities which are an unfortunate legacy. We continue to work closely with central agencies on these issues.

The recent Public Service Commission report on interventions with respect to the management of staffing at the OPC since June 2003 made public the results of the review of staffing files and confirmed that individuals, whose appointments were reviewed, were qualified for their existing positions. The report also concluded that progress had been made in addressing recommendations of the audit.

We continue to work with the Public Service Human Resources Management Agency on ongoing classification reviews and are nearing completion of this exercise. A total of 75% of the total classified positions have been reviewed. To date, we have maintained the level of 85% of the positions reviewed—six positions were downgraded and five positions were upgraded.

Since the audit carried out in 2003-2004, we have made a number of changes to improve how the office is run and to address the quality of our workplace.

● (1540)

We have engaged employees in a strategic planning exercise which has led to the development of a Report on Plans and Priorities. The process also contributed to the development of an HR strategy/action plan which was communicated to staff in April.

We have implemented an instrument of delegation of HR management authorities to clarify managers' accountabilities and initiated monthly communication to staff on employee mobility within the organization to support greater transparency.

We have designated an Assistant Commissioner as Internal Champion for Values and Ethics. That is my colleague here on my left. We have organized information sessions on the Values and Ethics Code of the Public Service and delivered a set of seminars on value-based staffing, performance management and harassment prevention.

Our Office has also created a Union Management Consultative Committee and a Health and Safety Committee to resolve mutual issues of concern.

Because of the length and complexity of the classification review process, it has seriously delayed the timing of the process for the organization of competitions for permanently staffing our vacant positions including several key management level jobs.

We are conducting a workforce analysis which will assist the organization in developing its staffing strategy, which will be submitted to the Public Service Commission for approval in principle. We expect to finalize a draft staffing strategy to the PSC by the end of December.

● (1545)

[*English*]

I would like now to turn to the question of the main estimates. As you are aware, the Office of the Privacy Commissioner has been funded to protect the data protection rights of Canadians in accordance with two federal statutes. The Office of the Privacy Commissioner has an annual budget of about $4.7 million to implement the Privacy Act in order to investigate complaints from citizens, to respond to public inquiries, and to carry out compliance reviews. This budget—and I would like to draw your attention to this—has not been substantially modified for years now.

Under the new Personal Information and Protection of Electronic Documents Act, PIPEDA, the office was provided with a budget of $6.7 million, which sunsetted last year. It was renewed for one year. and was tabled to Parliament in the supplementary estimates (A). This has resulted in the fact that the main estimates only reflect requirements under the Privacy Act and do not currently reflect the funding needs of this office to address the legislative requirements under PIPEDA. Our office is working in accordance with Treasury Board Secretariat requirements to determine the appropriate level of funding required to carry out our responsibility under the two acts.

As well, the office assumed additional responsibilities under the 2002 Treasury Board policy on privacy impact assessments, for which it has never been funded. To carry out this exercise, we have agreed to an A-base review of the office's operation, which will include a business process review of our investigations and inquiries functions, which accounts for a significant portion of our resource utilization.

In 2005 we will work with the Treasury Board Secretariat on a submission for long-term funding solutions and options, with the mutual objective to secure an adequate level of funding so that we can fully implement our institutional renewal strategy to further strengthen our human resources practices and reposition our core operations and functions to meet the ever-increasing complexity of privacy issues in both the public sector and the private sector.

As you may know, this is a pivotal time for the Office of the Privacy Commissioner. We must continue to demonstrate value in educating and informing Canadians about the importance of privacy. We must renew confidence in our office's capabilities to address the complexity of these issues.

I believe we are making slow but nevertheless steady progress toward that goal. I would like to, at this time, commend our office's staff for their professionalism and their dedication while doing their best to serve the Canadian public in innovative ways. During this year we have laboured under many unprecedented challenges, but I am confident that we will continue to emerge as a more effective organization and parliamentary agency.

I thank you very much for giving me the opportunity to make this presentation. I would be very happy to answer your questions, as would my colleague.

The Chair: Thank you.

We'll go to questions now. The first round will start with Russ Hiebert.

Mr. Russ Hiebert (South Surrey—White Rock—Cloverdale, CPC): Thank you, Mr. Chair.

Thank you for being here today, Ms. Stoddart. I appreciate your taking the time to address this committee.

I have a number of privacy concerns related closely to the nature of my constituency. British Columbia has a variety of reputations, but one of them has to do with marijuana, particularly in an area of the province where it's highly prolific.

The recent decision from the Supreme Court of Canada has raised some concerns about privacy related to this issue. I'm referring to the Supreme Court of Canada's decision in October that allowed the RCMP to use heat equipment to investigate whether or not homes were being used as grow operations. This was a surprise decision, a unanimous decision, from the Supreme Court of Canada overturning an Ontario Court of Appeal decision.

To what degree do you agree with the court's decision to give police the ability to investigate homes, using this infrared equipment? Do you think it impinges upon Canadians' privacy?

● (1550)

Ms. Jennifer Stoddart: The honourable member has raised an important question. I think you're referring to the Tessling decision. This was, I think, in Canadian jurisprudence a new way of interpreting privacy protections and concern. My office was very interested in the decision and I think somewhat surprised by the approach that was taken there. It is new, and as you pointed out, it did overturn the Ontario Court of Appeal's decision.

As I remember—I haven't read it for several weeks—the Tessling decision points out that privacy is to be analyzed in the particular context of its use, and particularly in relation to a territorial dimension that privacy would have. It distinguishes the traditional legal approach of the home per se with the fact now that we can read information on the exterior of the home.

As I remember, the Honourable Mr. Justice Ian Binnie elaborated on that distinction to say that the traditional jurisprudence on the home per se, then, was not directly applicable in this case. He talked about how, with this particular technology, we could read the emanations of the home.

As I said, this is a new interpretation. As you probably know, it contradicts, I think, a majority opinion by Justice Scalia in the American Supreme Court. I think the comment of our office is that we will wait to see how this is played out in particular contexts. Mr. Justice Binnie does take pains to say that in the facts of that particular situation we are not looking at the home, we are not looking at what happens inside the home, rather we are simply reading, in a cold climate, the temperature of the exterior of the home.

I think a key point is that he says this information was used with evidence that the police—as I remember, the RCMP—had previously. So this would seem, then, to preclude some kind of mass approach of going down the street and seeing whose homes were the hottest and concluding facilely that they were grow operations, but that this was the final bit of evidence in a series of evidence that began with some information from informants.

That's a long answer. I was just trying to remember the details of that case as you mentioned it. It is a surprising decision, and we will continue to watch that and see how it's applied.

Mr. Russ Hiebert: You have a great memory for the details of the case.

One element that perhaps may be a bit confusing is the fact that Justice Binnie did suggest that it wouldn't be in isolation, that this evidence could be taken in isolation and that perhaps the RCMP could in fact patrol the streets looking for opportunities to investigate. But I don't sense you taking one position or another on the Supreme Court of Canada's decision.

I won't press you on that, but my next question would be, how far do you think the police should be allowed to go in this sort of surveillance, or should there be other tools that the police should have to do their jobs?

I have one final related question. Where do we find the balance between the needs of the police to investigate crimes, or in this case to prosecute, versus the privacy of Canadians? That's the overarching question here.

Ms. Jennifer Stoddart: Well, the honourable member knows that is the question we continue to ask ourselves and ask of the government in many, many situations. You've raised one particular fact situation. It is difficult in our society, struggling to find the right balance.

The balance is, of course, always in the context of the particular technology, the particular operation that is being used, so I don't think there's an overall answer. There's always a more precise answer, but I think what we're concerned about is that our society is increasingly turning towards surveillance technology and that the balance then is imperceptibly shifting, and we rarely go back and justify—up until now, anyway—the increase in security, in crime fighting, or in anti-terrorism implications that have been gained because of this shifting balance.

To try to answer your other question, my recollection of the case was that you had to have some other significant proof. It's hard for me to reply to your second question, because I had understood that you cannot just read the heat on people's houses. The police have to have other significant material evidence in order to use that.

● (1555)

The Chair: The time is up.

Monsieur Laframboise.

[*Translation*]

Mr. Mario Laframboise (Argenteuil—Papineau—Mirabel, BQ): Thank you, Mr. Chairman.

My first series of questions will obviously concern the 2004-2005 Main Estimates. From what I understand, you're not requesting a budget adjustment. So you're theoretically satisfied with the amounts that have been allocated to you in the Estimates, and you may request more in 2005-2006. Have I correctly understood?

Ms. Jennifer Stoddart: That's correct.

Mr. Mario Laframboise: However, in the Report on Plans and Priorities that you signed in April of this year, you stated:

> My most immediate priority, however, has been to lead the Office's institutional renewal by strengthening its management processes, particularly as they relate to human resources and financial management—planning, budgeting, reporting and control mechanisms.

And you say further on:

> I believe that we are well on our way and I anticipate that by summer of 2004, most of these legacy issues will be behind us.

However, the report submitted by the Public Service Commission in October states:

> ...the OPC has not yet... put in place the required reporting and monitoring/control system.

You anticipated doing that for this past summer, but you hadn't yet completed everything in October. What prevented you from doing the work you proposed to do?

Ms. Jennifer Stoddart: Sir, there you're addressing a central theme to the operation of the Office over the past year. As you clearly know, we wrote that in March 2004. We're still optimistic about what we can and think we can accomplish. Over the past 12 months, despite our optimism and efforts to implement all these reform processes, we saw that regularizing the situation at the Office was taking a little more time than we had anticipated. So when summer arrived, we still had a number of things to do. That's what is reflected in the Public Service Commission report.

Mr. Mario Laframboise: When do you anticipate... I suppose you won't make anymore promises about what you want to do. What's the crucial issue right now? Is it staff restructuring?

Ms. Jennifer Stoddart: A number of problems are delaying renewal of the Office. Our organization has been and is still undergoing investigations, audits, reviews and trusteeship processes by all of Ottawa's major agencies at the same time. The cumulative effect of all that has affected our efficiency and effectiveness and progress. I don't know whether I need to remind you that we have had the Public Service Commission, the RCMP, which didn't leave until April, and the Auditor General, twice. She has just completed her report, which was presented at the same time as our annual report.

What's been the hardest to live with day to day has been the review of the classification levels of virtually all employees. It's a fairly painful and lengthy process. Employee participation in the process is encouraged, and they obviously want to take part in it. That's the second major factor delaying reconstruction of the Office. People left after the unfortunate events of June 2003, and there's also the usual turnover in a government organization. Before staffing a position, you obviously have to ensure that the classification is correct. That's not an easy task.

● (1600)

Mr. Mario Laframboise: How many employees are you missing so that you can operate properly?

Ms. Jennifer Stoddart: Our strength should normally be 95 to 100 employees. We currently have 87 or 88.

Mr. Mario Laframboise: Does that prevent you from handling complaints? Is the number of service requests from citizens the same or increasing?

Ms. Jennifer Stoddart: We're still receiving requests, and I must say that has caused a lot of stress among staff. I'm mainly thinking of investigations and requests. For front-line information, I think we had six employees last fall. We currently have two, I believe. Investigators take turns helping their co-workers and answering the telephone and e-mails. We can't do it all.

We had to establish the classifications and restaff. That's perhaps one of the areas where it's hardest for staff. Consequently, there are more delays than we would like in answering public requests.

I should add, however, that we manage to conduct our investigations quite quickly. Investigations under Part I of the Personal Information Protection and Electronic Documents Act, which concerns the protection of personal information in the private sector, must be conducted in less than a year. That's being done. Investigations under the Privacy Act are conducted in four to eight months on average. However, some cases are outstanding.

Mr. Mario Laframboise: How many are there?

Ms. Jennifer Stoddart: As I remember, I would say there are approximately 200 under the Privacy Act and about 30 under Part I of the Personal Information Protection and Electronic Documents Act.

Mr. Mario Laframboise: How many cases do you handle each year?

Mr. Raymond D'Aoust (Assistant Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): May I clarify a point? We have 341 complaints under the Privacy Act. Under the Act respecting the Protection of Personal Information in the Private Sector, 95 complaints have to be processed.

Mr. Mario Laframboise: How many do you handle each year?

Ms. Jennifer Stoddart: I'll try to find the annual report to give you the exact figures. It seems to me we handled several thousand last year.

Mr. Raymond D'Aoust: It's stated on page 26 of the English version of the report that we handled more than 2,000 complaints last year. The figures are there.

Mr. Mario Laframboise: So approximately 20 percent of cases... This is a situation that you expect to resolve once you have all your staff.

Ms. Jennifer Stoddart: Absolutely.

As I said in my remarks, we are reviewing the methods we use to prepare our long-term funding submission for the work we do under the legislation governing the private sector. We hope to start doing that this winter and next year.

Funding for the work we do under that act has been granted to us for three years, as I mentioned. We are somewhat stuck in the middle. Consequently, Treasury Board is encouraging us to review our processes before establishing our permanent funding level.

In view of our Office's legacy, over the first three years of the act's implementation, we may not have exercised all the necessary administrative control or verified the effectiveness of the approach developed to implement the new act. That has to be done.

● (1605)

[*English*]

The Chair: Sorry to interrupt, but your time's up.

Mr. Lee.

Mr. Derek Lee (Scarborough—Rouge River, Lib.): Thank you.

I thought your comments were very useful on the Supreme Court decision. I found the decision to be very rational and consistent with my view of the universe. I hope it helps the Office of the Privacy Commissioner in its work, because it occurs to me that the citizen is quite capable of assessing what goes on in a private residence.

From the outside, we routinely take note of whether the lights are on or off sometimes, a barking dog, loud music, the smell of smoke, or a Geiger counter picking up radioactivity—and now we're picking up heat. All of those things don't allow us to know exactly what's going on in the house, but they do cause us to make judgments about whether further steps are needed. That would include the police.

So I did find your comments helpful, although I detected a note of skepticism. I'm just weighing in on the side of the court here. It may influence decisions in other countries.

In any event, I was curious about why we continue to maintain a fiction in the funding between the Privacy Commissioner's work and the work under the PIPEDA, as you call it. The PIPEDA funding was sunsetted. It's been renewed. Surely this isn't going to go on forever.

Was it the view that you would be able to fold the funding under the new statute into the normal Privacy Act functions and we wouldn't have to have a bifurcated funding mechanism?

Ms. Jennifer Stoddart: I'm not sure...to answer the honourable member's question.

Mr. Derek Lee: That's okay. You can speculate—but you don't have to speculate, because that's not your job.

Ms. Jennifer Stoddart: Yes, I think somebody in Treasury Board might have a better idea of that.

Mr. Derek Lee: All right.

Could we just note, Mr. Chairman, we're curious that...if we're going to sunset and renew, sunset and renew, why don't we just fold the funding into the whole office operations so we know exactly what we're spending there?

Is that okay, Ms. Stoddart?

Ms. Jennifer Stoddart: Certainly.

Mr. Derek Lee: In your report, you indicate that the big attractions for complaints are the banks and financial institutions. I shouldn't say just banks, but financial institutions are the big draw for complaints. Do you have any idea why that is? Is it just an area of heightened sensitivity in relation to privacy, or do they need more changes to the way they do their work?

Ms. Jennifer Stoddart: I believe I posed that very question when I took over this job, as I hadn't recently worked in the federal sector and had noticed that too. My staff members, who of course are involved in every complaint, and so on, said that in general, the sense of our office is that the banking sector is in fact doing quite well in protecting privacy.

However, there are a couple of things in our lives that we generally have heightened privacy concerns about. One is our health, and one is our money. That's why, for example, the Income Tax Act has special privacy protections that other legislation doesn't.

The bankers have a long tradition in privacy protection. Part of the reason we traditionally do business with them is that they have a history of keeping our affairs private. However, there are slip-ups. I say there are players in the banking sector that have a greater commitment to privacy than others. There are ones that have more familiarity with this as a value in the banking world. If you go to a bank and there's one privacy slip-up, of course you're going to be very concerned.

So I think the public is quite sensitized and quite ready to come to us on that issue. I don't think the banks are necessarily doing worse than another sector; generally they're doing quite well. But I think the public is concerned about the privacy of its financial information.

● (1610)

The Chair: Thank you.

Mr. Broadbent.

Hon. Ed Broadbent (Ottawa Centre, NDP): I too welcome you.

Ms. Jennifer Stoddart: Thank you very much, sir.

Hon. Ed Broadbent: You expressed in your opening statement some concerns regarding information about Canadians that should remain private perhaps crossing borders, I assume to the United States, in terms of certain issues that have been raised.

As you know, the Privacy Commissioner in British Columbia has said, with reference to the U.S. Patriot Act, that it “knows no borders”, i.e., it applies to Canada. As a result, the British Columbia government brought in legislation intended to deal with the situation, at least as it affects the public sector.

My question to you is, does federal legislation sufficiently protect Canadians in the domain of transfer of cross-border information, and with specific reference to the U.S. Patriot Act?

Ms. Jennifer Stoddart: Thank you. That's an extremely important question.

I'll begin by saying, in answer to whether we have adequate Canadian legislation, yes and no. You've already highlighted that we've now applied two acts for the last year. One is a piece of legislation that dates from 1982-83. We pointed out at the time Commissioner Loukidelis' report was tabled—and we joined him in many of his recommendations to the federal government—that the Privacy Act is not up to the task of protecting Canadians' information, of setting an adequate standard in the face of this new phenomenon of the international circulation of information.

The PIPEDA, the Personal Information Protection and Electronic Documents Act, which is much more recent and was adopted by Parliament in spring 2000, does have those kinds of safeguards. We pointed that out in our brief to Commissioner Loukidelis' inquiry. It has the accountability principle. It says that what we call the data controller—the person who has control of the personal information—must ensure that it will be treated according to the standards it would be treated with in Canada, before sending it on. So you have recourse then, technically or ideally, under this legislation against the Canadian entity that sent information somewhere else.

We also have in PIPEDA a fairly strong whistle-blower provision, which we also highlighted. If people see, in the course of their activities or their work, information being incorrectly accessed, they have a certain amount of protection if they come forward with this.

So we took this opportunity—and I've been doing this over the last few months, starting last spring—to remind the government that it should think of moving ahead with bringing our Privacy Act up to date with the modern world of information circulation.

Hon. Ed Broadbent: To pick up on your reference to PIPEDA, paragraph 7(3)(c) of the act allows an organization to disclose personal information where it is required to “comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information”. The word “domestic” isn't in there. Has this not led to information being transferred outside Canada that perhaps should not be? Could this be dealt with by inserting the word “domestic” before “subpoena” and “warrant”?

Ms. Jennifer Stoddart: As I remember, the opinion of our office in the brief was that this is usually interpreted, according to the normal rules of interpretation, to mean domestic, to mean a Canadian court, and the normal legal rules would be that the order of a foreign court has to be—in civil law we say homologated—adopted by a Canadian court. Foreign jurisdictions cannot just enforce their own orders here; they have to go through a Canadian process by which this is approved and adopted by a Canadian court. We took that particular part of PIPEDA to mean that applies to a Canadian court.

● (1615)

Hon. Ed Broadbent: You've taken it to mean that, but for example, in the Maher Arar case is there any reason to believe that others haven't interpreted it that way?

Ms. Jennifer Stoddart: I really can't comment. I don't know enough about the Maher Arar inquiry, and it is before a judge, so I don't think I should comment on it. Certainly, it is clear from Commissioner Loukidelis's report that there are various interpretations possible of the reach of Canadian legislation, of the strengths of the protection of Canadian legislation, and of the extraterritorial application of the Patriot Act. That is something I think no one can really predict accurately, and of course, it is something about which we can't really know if it is happening.

Hon. Ed Broadbent: To go back to the action that the B.C. government took in the context of existing federal legislation, it believed the existing federal legislation, from the point of view of protecting Canadians, was not adequate. I presume that you've had a look at the B.C. legislation. If I heard you correctly, the two acts you referred to are the Privacy Act and PIPEDA, so between them, although you said the Privacy Act should be updated in certain ways, on the whole, PIPEDA is dealing with this safeguards issue. If that's so, why did the B.C. government have to act?

Ms. Jennifer Stoddart: I believe the B.C. government acted in the area that was of provincial jurisdiction. The concern that arose in B.C. had to do with the actions of the B.C. government, so this would not be something in which either of the federal acts would necessarily apply.

The Chair: Mr. Bains.

Mr. Navdeep Bains (Mississauga—Brampton South, Lib.): Thank you very much for coming here today.

I want to follow up what Mr. Broadbent was saying in respect of the U.S. Patriot Act. I want to pose a hypothetical, if you could help me out here. As you know, there's a trend for outsourcing a lot of information nowadays. Say there's a company in B.C., a bank for example, and say the database is physically held in the United States of America; that's where the information is stored. Is that subject to the U.S. Patriot Act, and would that information be available to the United States?

Ms. Jennifer Stoddart: Yes, and we said in our brief to Commissioner Loukidelis—it's on our website—that any information that is sent to the United States is normally subjected to American special legislation, like the Patriot Act.

Mr. Navdeep Bains: So at present all the databases that exist in the United States with information that pertains to many Canadians, possibly some of us, because we do banking with many of the various banks there, potentially are under the U.S. Patriot Act, and they can access that information. Have you any recommendations that could prevent that from happening here, from a Canadian perspective?

Ms. Jennifer Stoddart: No, I think as a matter of law, if the information is in that country it is subject to that country's laws. The converse is true. Information processing flows both ways. We have information on people from other countries that is processed in Canada and is then subject to Canadian laws.

We have a fact sheet on our website that talks about what people can do—steps they can take to protect their personal information in a context where information circulates widely and globally. I don't think, however, we can suggest any way for American laws not to apply within the United States.

Mr. Navdeep Bains: If we physically move our database from the United States, or whatever, if the out-source company were in Canada, obviously they would be subject to Canadian law, but is there no way, in any shape or form, that we can create some sort of clause in our agreement that says that law does not apply to our information in the United States?

● (1620)

Ms. Jennifer Stoddart: I would be very surprised. We did not take the position that it was possible. Again, if you put yourself in—

Mr. Navdeep Bains: I thought the change the B.C. government proposed was in light of that concern primarily.

Ms. Jennifer Stoddart: My understanding of what the B.C. government is proposing is that information processed in British Columbia benefit from safeguards within British Columbia. I don't remember that it has an extraterritorial reach.

Mr. Navdeep Bains: I have another quick question for follow-up.

As we know, there's a great deal of information nowadays with the dissemination of technology. In August 2000 the former Minister of Justice, Anne McLellan, announced that her officials had begun a comprehensive review of the Privacy Act to ensure its continued relevance in the age of rapid technological advancement. What's your knowledge of the status of this review, and if there is any review taking place, what's your role in this?

Ms. Jennifer Stoddart: I guess our role is very general for the moment. Anne McLellan's new department is just forming. We've met with them several times.

Mr. Navdeep Bains: This was in her capacity as the Minister of Justice, though, in 2000.

Ms. Jennifer Stoddart: Oh, excuse me. This was in 2000?

Mr. Navdeep Bains: Yes. Just to again clarify, this was a comment she made in 2000, asking the Privacy Commissioner to review the Privacy Act to ensure its continued relevance in the age of rapid technological advancement. This was a recommendation she made in 2000.

Is this review taking place? If it is, what's your role?

Ms. Jennifer Stoddart: To the extent of my knowledge, but the assistant privacy commissioner may have something to add, there is no full-scale review of the Privacy Act at this time. This is something, as I said to another honourable member, that I have called for. We think it should be looked at very seriously. I'm not aware that there is any major review, but I'm meeting with Ms. McLellan's successor, Minister Cotler, later this month to urge him to begin a review of the Privacy Act, which has been the subject of many recommendations over the years.

Am I correct?

Mr. Raymond D'Aoust: Yes, you are correct. The office did submit a brief to the Department of Justice—you are right—containing more than 100 recommendations to amend and revise the Privacy Act. As I understand it, there was some discussion, but no amendments or reform of the act actually ever occurred as a result of those discussions. We're going to be reinitiating those discussions with the Department of Justice soon.

The Chair: We'll keep up on that one.

Mr. Hanger.

Mr. Art Hanger (Calgary Northeast, CPC): Thank you, Mr. Chairman.

Thank you, Commissioner, for coming before the committee.

I note in your annual report to Parliament one statement I would like some clarification on, and I'll have another question to follow.

It says your office serves as a source of in-house expertise providing assistance and advice to both public and private sector institutions. What private sector institutions would you provide advice to?

Ms. Jennifer Stoddart: It's a wide variety of private sector institutions, particularly since we've had responsibility for PIPEDA, and particularly because since January 1, 2004, this law applies across Canada to commercial activities, unless the province has its own substantially similar legislation. We have been literally inundated with requests for advice through phone calls, e-mails, letters, and so on, and our staff, including our legal staff, worked very intensely, particularly at the beginning of the year, to provide advice on how this law applied. We also developed a lot of specialized material on our website.

So there is a variety of institutions there.

Mr. Art Hanger: And many of these institutions, I gather, would have investigative bodies of one type or another?

Ms. Jennifer Stoddart: Do you mean their own internal investigative bodies?

Mr. Art Hanger: Yes. For instance, the bankers have an investigative body.

Ms. Jennifer Stoddart: Yes, some of them would.

Mr. Art Hanger: The Insurance Bureau of Canada has an investigative body. It's possible some power or utility operations have an investigative body.

● (1625)

Ms. Jennifer Stoddart: Yes, some of them would.

Mr. Art Hanger: In that line, I know that under subsection 7(3)—paragraph (d), I believe it is—non-consensual disclosures of private information can be made to these investigative bodies or by these investigative bodies to other agencies. In other words, the movement of information can exist. I understand that's what paragraph 7(3)(d) says. Is that correct?

Ms. Jennifer Stoddart: I believe so.

Mr. Art Hanger: Okay. This seems to be posing a problem for some of the agencies. One individual who is involved in investigation commented that he is very much hampered by the interpretation of this particular section and says—I'll use his words—"I find it difficult to understand as the intent of the laws from a strictly layman's point of view was designed to protect the privacy and personal information of the public (the law abiding individual), not protect the organized criminal element..."

This is the roadblock they are finding themselves facing. One of my colleagues just brought up the matter of grow ops, for instance. Organized criminal activity is very intense. It's not only running in British Columbia; it's in Alberta here now. It's causing millions and millions of dollars to flow through into organized criminal activity and it's also destroying a lot of property.

The problem that exists is that the police may make reference to such an operation when they take down a grow op house, for instance, and make it known through the media. They will not release any official statement, because they're fearful of lawsuits. At the same time, electrical companies may know of concerns relating to criminal activity at a residence—and if you understand how these grow ops operate, they'll bypass electrical checkpoints or, as the case is now, not even bypass; there are just huge bills being run up—but they cannot pass that information on to police for fear of a lawsuit. And it all relates back to privacy.

What is wrong with this picture? I can understand the viewpoint being expressed by organizations about whose side of the law the privacy act is really supporting. Whose side is it really benefiting if criminal organizations are able to operate almost with impunity?

The Chair: Please give a quick answer, if you can.

Ms. Jennifer Stoddart: I hadn't heard that perspective , I must say, or the problem the honourable member is raising. In relation to PIPEDA, I hadn't heard it was a problem for police investigations, because usually we interpret it as being an exception in terms of police investigations, if they're conducted in the proper way.

Some of these things, such as electricity, would be covered by your provincial legislation, I think. There's certainly nothing that stops the police or investigative body, if they have the proper procedures, from getting this kind of information. We often hear that privacy prevents us from doing this or that. If the police have some reason, they can get a warrant from a judge to examine this information, and certainly privacy laws are not a bar to that.

The Chair: Art, you'll have to ask it in another round.

Monsieur Boulianne.

[*Translation*]

Mr. Marc Boulianne (Mégantic—L'Érable, BQ): Thank you, Mr. Chair.

Welcome, Ms. Stoddart. We met previously in a very different setting. I would also like to welcome Mr. D'Aoust.

One of your main objectives is the Office's efficiency and effectiveness. You have conducted a strategic planning exercise in this area. You've also involved your employees. That's produced results. You have identified priorities, which has enabled you to develop a strategic plan and an action plan. I would like to hear what you have to say on that. Can you also tell us how that has improved the Office's efficiency?

● (1630)

Ms. Jennifer Stoddart: The fact of conducting that exercise?

Mr. Marc Boulianne: Yes, the fact of conducting that exercise. Can you also tell me how the exercise was carried out?

Ms. Jennifer Stoddart: The exercise was carried out this past January. Approximately one-third of employees were withdrawn from their normal activities and worked with a facilitator to consider the Office's orientation, mission and objectives. Then an internal committee was established consisting of employees interested in these issues and headed by a manager. They helped us to find our three major objectives. We also had the contribution of an outside advisory committee, which made comments on those objectives. That's it for the process.

Now how does that help us be more effective and efficient? Based on these objectives, we expect every manager, in each of the branches, to develop some objectives supporting the main objectives. This may be something that goes without saying, but I believe that, in the previous administrative confusion, this was something that was not done very much, or even at all, in previous years.

So it's a whole exercise in which we're trying to organize coherently the objectives of the entire Office, those of each of the branches and thus of the managers, and those of employees, so that we can all work to achieve our main objectives.

Have I answered your question?

Mr. Marc Boulianne: Yes.

Last week, I met a voter who had come to complain about the fact that her date of birth was very often being used inappropriately, without her permission, for all kinds of reasons. She had the impression it was a violation of her privacy, and she didn't feel there was any protection against it.

Have you received a number of complaints concerning the use of birth dates?

Ms. Jennifer Stoddart: Yes. There are some on birth dates and others on social insurance numbers.

Mr. Raymond D'Aoust: We receive them and we process them, but I couldn't tell you the trend in that regard. Of course, a birth date, combined with name and other information, makes it possible to identify an individual accurately.

Mr. Marc Boulianne: Are there any criteria for the use of a birth date? If it's misused, that indeed becomes a violation of privacy. Can it be used like that, at every turn? Especially birth dates?

Ms. Jennifer Stoddart: I don't believe there's an act preventing the use of birth dates as a classification organizer.

In our annual report, we made a fairly interesting comment on the use of social insurance numbers following a complaint. That's somewhat the same problem. Social insurance numbers are a little more regulated by the federal legislation, and people have to give their consent. There's nothing preventing organizations from requesting them, or people from giving them.

We try to make people aware of this issue. We tell them to beware to whom they give these major identifiers, social insurance numbers and birth dates. They are widely used, and we tell people that they are not required to give them to everyone. There are few situations in which they are required to do so, and we cite them.

Mr. Raymond D'Aoust: That's on pages 80 and 81.

Ms. Jennifer Stoddart: Few provisions in Canadian legislation require people to give them. To my knowledge, there's nothing on birth dates. I don't think so.

Mr. Marc Boulianne: Thank you.

[*English*]

The Chair: Your time's up.

Mr. Tilson.

Mr. David Tilson (Dufferin—Caledon, CPC): Mr. D'Aoust, you indicated that there had been 100 recommendations to the justice minister. Can you undertake to give us those recommendations?

Mr. Raymond D'Aoust: I don't have the detail here with me.

Mr. David Tilson: I understand, but could you undertake within the next period of time to get us that information?

● (1635)

Mr. Raymond D'Aoust: Sure, we can give you an overview.

Mr. David Tilson: Thank you.

I appreciate your reducing your introductory remarks, Ms. Stoddart, to writing. It's very helpful, and I am interested, as Mr. Lee was commenting, on the funding part of it between two pieces of legislation.

Can you tell us how your office gets its funding? How does it obtain its funding? Do you go cap in hand to the Treasury Board? What do you do?

Ms. Jennifer Stoddart: Well, it's an exercise between agencies. Recently, I guess we've gone cap in hand to Treasury Board, because the amount we were originally granted for the years between 2000 and 2003 lapsed. I guess it ended or lapsed at the beginning of this year; therefore, yes, we did in fact go cap in hand, but of course Treasury Board was very sensitive to our situation.

This three-year funding lapsed, so we agreed it would be carried over one year, and in fact it's being carried over automatically a second year. During this second year we will apply for permanent funding, having made our case. It's called our business case. So it will probably be the spring of 2005 by the time we get all the—

Mr. David Tilson: And the Privacy Act, is it similar?

Ms. Jennifer Stoddart: The Privacy Act is recurring funding, with funding recurring for quite some time at the same level. From the indicators we have, it is insufficient, because historically some of this PIPEDA money was used to fund Privacy Act activities. This was one of the administrative challenges, to try to sort this out in our activities.

We believe the level of funding for the Privacy Act, given Canadians' interest in privacy issues and particularly given the whole range of technological issues before our office, and on which we have to build our analytical capacity, is insufficient.

Mr. David Tilson: Now, you mentioned in your comments that your office is working with the Treasury Board Secretariat "to determine"—in your words—"the appropriate level of funding required to carry out our responsibility under the two acts". Has that been concluded?

Ms. Jennifer Stoddart: No, it's not.

Mr. David Tilson: When will it be concluded?

Mr. Raymond D'Aoust: It will be concluded in the fall of 2005, when we get a decision.

Mr. David Tilson: Okay. Where I'm going with this line of questioning is that I sense you're saying you don't have enough funding for either piece of legislation. You haven't said that, but you've got a backlog, you're talking about the budget under the Privacy Act having not been modified, and you're talking about the other budget being sunsetted. You're skirting around the issue.

Is there a problem, or is there not a problem?

Ms. Jennifer Stoddart: Well, we don't want to skirt.... I'll try to give you a direct answer, but it's kind of a circumstantial answer.

Right now, I think a public accountant would say to us, "You're not in a position to spend all of your budget", and I can't quarrel with that. Why can't we spend all of our budget? It's because we can't staff fast enough, for all the reasons I was explaining to some of the honourable members, because we had to do all this housekeeping and we had to revise the classifications. So in fact, right now, because we have so many jobs that are not staffed, we can't say today that we are lacking money. That's a very unusual situation, and we hope to get through it.

However, and certainly long term, we foresee that our funding is inadequate. But we have to build a case on it, because if I say that today to Treasury Board, they're going to say, "But look, you can't spend all the money you have because you've got all these jobs that are unfilled". In order to build a case, it takes a fairly elaborate analysis, both under the Privacy Act and PIPEDA, going forward from the amount of money we have.

But right now, I can tell you the experience of the last few years of the office is that we're spending money from PIPEDA just to do our complaints under the Privacy Act, and to try to do minimal public education activities about Canadians' privacy in the public sphere, and so on. That takes money from PIPEDA. As you pointed out, if we had that money, or more, we could spend it, once we get through these personnel management hurdles, on faster complaint processing, public education, reaching out across Canada, and so on.

● (1640)

The Chair: Time is up.

Mr. Hiebert.

Mr. Russ Hiebert: In your opening remarks, you commented on your responsibility to draw Parliament's attention to certain issues and to inform Canadians about certain issues. You make reference to radio frequency identification devices, RFIDs. As we all know, these are microchips that are currently being used to track things such as pallets. I hear they're now being used on products, pets, livestock, and other things like that.

There's the example of what would happen if one of these microchips was to be used in a sweater; you purchased it with your credit card, left the store, and later returned. They'd have tracking devices to show you've returned and would track where you go in the store, who it is that you are, and when you purchased the sweater. When I hear stories like that, I become particularly concerned about the potential loss of privacy to Canadians.

I now understand there has been an application to test these tags in humans. It's being proposed as a security biometric device or technology. Again, I think there are serious risks associated with this sort of technology, not only on products but also on people. Following along the *Spider-Man* principle, with great power comes great responsibility. Certainly, with great amounts of data comes greater responsibility as well.

Could you comment in more detail than you did in your opening remarks about the proper balance that should be struck between consumer privacy and retailers collecting data or, in this extreme example, using this information to track people?

Ms. Jennifer Stoddart: This is an issue that is of great concern to us, biometrics generally. RFIDs, more specifically, are a new type of biometric. One of the things that we're attempting to do is build up the office's technological capability to monitor these new devices. At the rate at which technology is developing, there's a new one every six months, a new device or application or technology coming forward. This again is a long-term process. Given our staffing problems, we don't have that kind of technical expertise, but I hope to be able to get it within the next few years.

One of the concerns we have is the use of RFIDs in public documents; for example, its possible use in passports in order to try to make the passport a unique document and thus prevent falsification. We are in touch with the Passport Office and have made our concerns known to the Passport Office. As they go forward and test new types of passports with biometrics for the Canadian public, I believe we've asked for a privacy impact assessment to be done and forwarded to our office. We have not yet received this.

In the long term, I think the question you raise does not yet have a clear answer on the way to prevent, for example, RFIDs being put into humans, tracking humans like merchandise, and so on. This is one of the things we're going to give a lot of attention to in the coming years.

Is this something like genetic engineering, for example, to take technology in another area of human existence, where it raises such fundamental moral and ethical questions that in fact Parliament should have some kind of special law about the use of RFIDs, the limitations, and so on? I don't know, those are things we're following.

Mr. Russ Hiebert: I do look forward, with great interest—

The Chair: You're way over the time limit.

Mr. Broadbent.

Hon. Ed Broadbent: Thank you.

I want to go back to the extraterritorial issue that you raised about Canadians not having the right to impose Canadian requirements on the U.S. Once the U.S. had certain data about Canadians, it was within U.S. territory. As we know, because of the Patriot Act, extraterritorial is working in the opposite direction right now, i.e., American law applying here.

If I understand it correctly, the CIBC case in which a Canadian bank is using an American processing company means not only Canadian companies doing business with CIBC, but every user of a CIBC Visa is now subject to the provisions of the U.S. Patriot Act and all that information is now available to the U.S. Am I right?

● (1645)

Ms. Jennifer Stoddart: That's my understanding.

Hon. Ed Broadbent: Isn't this a serious problem?

Ms. Jennifer Stoddart: It is a serious problem, but it is not a unique problem. If I can point it out to the honourable member, it would appear to us—although we have no clear facts and figures—that Canadians have, for possibly many generations, been sending their personal information to the United States, as Canada processes personal information of Americans here, depending on the configuration of certain industries. This is not a new development. Given the rules of international law, then, the law of the place where this processing is taking place usually applies.

The new interest—because I think Canadians have been unaware of this—is that this is a wake-up call for Canadians to think about where their information is going and who they're giving it to generally. I don't think that's just an issue of whether it's here or in the United States. We understand that information in all industrialized countries is now circulating very rapidly between those industrialized and democratic countries, but between other countries, too, where this information can be processed.

We really have an issue that is much larger than an issue of our information being processed in the United States, which is not a new phenomenon. It is the issue of how we develop privacy standards in a globalized economy in which our own personal information is circulating.

Hon. Ed Broadbent: If I understand what has happened, it is a new phenomenon. That is to say, if I've understood what you've said, yes, there have been aspects of this transformation of Canadian data or private data about private individuals in the past, whether it's to the U.S. or some other foreign country, but in one sense this seems to be, to me, a kind of exponential extension of this.

As a matter of fact, I do have a CIBC Visa card. I'm sure most Canadians across this country would be quite surprised to know that all kinds of personal information about me, simply because I'm using that CIBC Visa card, can be transferred to the U.S. because of existing U.S. law—in this case because CIBC happens to use a U.S. processor.

Is there no way we can take steps in Canada to contain this information within our borders?

Ms. Jennifer Stoddart: That's certainly something that can be looked at and can be debated, but I would simply take the opportunity to remind you that there is a massive exchange of information between Canada and other countries, notably the United States.

The Parliament of Canada could pass laws that would prevent the exportation of our personal information outside of Canada—

● (1650)

Hon. Ed Broadbent: Wouldn't that be a good thing?

Ms. Jennifer Stoddart: You, as parliamentarians, would have to look at all the aspects.

In a world in which there's a globalized economy, my understanding, from talking to various specialists, is that we also process information that comes from other countries too. Canadian companies, or perhaps American companies with Canadian subsidiaries, process information that comes from the United States.

One of the first, most practical things we can do—and something I met Minister Alcock on about a month ago—is to start looking at the personal information held by the Canadian government on Canadians and making sure the Canadian government itself has appropriate standards for that sensitive information in terms of where it's going, what the security and confidentiality arrangements are, and how it binds the organizations to which it would give contracts.

My understanding—

Hon. Ed Broadbent: I really mean it when I say I don't want to be rude—

The Chair: I don't want to be rude either, Ed, but you're way past time.

Mr. Lee.

Mr. Derek Lee: This is a very useful discussion, but my reaction is that Mr. Broadbent's questioning is potentially alarmist in the sense that it's suggesting—

Hon. Ed Broadbent: Banks share the concern.

Mr. Derek Lee: The concern is real.

Hon. Ed Broadbent: Why is it alarmist, then?

Mr. Derek Lee: I'm getting into a debate with Mr. Broadbent. I should be putting questions to Ms. Stoddart, but we can certainly discuss this.

It is suggestive that just because information is processed outside borders, it's not subject to security and privacy protections. Our security professionals in Canada are just as capable of accessing personal information stored and processed here, no matter where it comes from, under the aegis of a warrant or under the aegis of Canadian legislation, as American authorities would be down there. It doesn't mean that every time somebody ships data to Canada, it gets put on the front page of *The Globe and Mail*, and that every time that data is shipped from Canada to the U.S.A., it shows up on the front page of *The New York Times*. So while the issue is real, I think we'd be looking to the Privacy Commissioner for some guidance and leadership on it.

I don't second-guess the good-faith objectives of Mr. Broadbent in raising the question. The Privacy Commissioner in B.C. has done that. Of course we have to look at it.

I should ask you, Ms. Stoddart, who on this side, if it's not your office—I hope your office is looking at it, if you have the resources—is looking at the general protections for privacy for Canadian data that does make its way across the border routinely into the U.S.A. Is your office looking at that?

Ms. Jennifer Stoddart: Perhaps I could remind you and remind the previous honourable member, or inform him, that we do have a complaint about the very situation he was raising. This is under investigation, so I really can't comment on either its possible outcome—

Mr. Derek Lee: Why not?

Ms. Jennifer Stoddart: Because it's under investigation. That's a traditional protocol, I think.

Mr. Derek Lee: It's not criminal.

Ms. Jennifer Stoddart: No, it's not, but we don't have all the facts before us, as far as I know.

Mr. Derek Lee: We could go in camera. Would you care to deal with it there?

Ms. Jennifer Stoddart: No, because I honestly am not personally involved with that investigation. So at this point, I couldn't tell you any more.

Mr. Derek Lee: Okay, thank you.

Ms. Jennifer Stoddart: I think our investigations are also confidential by law, so we will carry those out. Because we will eventually make a finding on this issue, this will give us the opportunity to say something about this practice and the extent to which Canadian legislation does or does not respond to the concerns of the complainant.

The Chair: Time's up.

[*Translation*]

Mr. Laframboise.

Mr. Mario Laframboise: Thank you, Mr. Chairman.

On page 57 of the English version of your report, you say, with regard to the RCMP: ...we did have concerns regarding the agreements or arrangements governing the sharing of personal information between the RCMP and its IMSET and IBET partners. The matter has been the subject of ongoing discussions with the RCMP.

I see that 164 complaints against the RCMP were handled last year. You seem to say you have concerns about the way the RCMP proceeds. Is there a relationship between the complaints filed against the RCMP and the recommendation you make on page 55?

Ms. Jennifer Stoddart: I believe they are two different things, but there may be connections. However, with your permission, I'll ask the Deputy Commissioner, whose area that is, to answer you.

● (1655)

Mr. Raymond D'Aoust: We conducted audits at the RCMP in this area after some of their activities had been established following the events of September 2001. A number of components were audited to determine whether they complied with the principles of the Privacy Act. Their practices are sound on the whole. We produced a report on the matter.

However, there was one area where we wondered more about the need to formalize the privacy provisions further. That was the exchange of personal information that the RCMP does with partner agencies at the provincial, federal and even municipal level. The RCMP undertook to act on those findings.

Mr. Mario Laframboise: Do you have the staff you need to conduct follow-up? Obviously, when you let the RCMP and other organizations like that go, they get away from us. They won't report to you on their own. Do you have the necessary staff to ensure follow-up?

Mr. Raymond D'Aoust: Yes. We have a team of auditors who are keeping an eye on that. Of course, it's a small team. We're talking about four individuals. They are currently busy on a fairly important project in which they are examining information transfers by the Border Services Agency, for example. That's the project those people are focusing on right now. Of course, if we had more resources, we could do more follow-up, but we're definitely doing what we can. These are disciplined professionals, and the working relationship between our agency and the RCMP is quite good. I think the RCMP is discharging its responsibilities quite well.

[*English*]

The Chair: Time's up.

Mr. Bains.

Mr. Navdeep Bains: Thank you very much.

Commissioner, you mentioned that the protection of personal health information is fast becoming a significant privacy issue. You also mentioned wealth, which is another one we've discussed, the whole notion of banking and the information there. We've also touched upon some provinces creating their own privacy legislation, such as B.C. I get the impression—and on page 12 you alluded to this as well—that based on personal health information there are small patches of privacy legislation that different provinces have established across the country. Many people are concerned, including me, that there's a developing patchwork of privacy protection in this field across the country and that we might require this to be harmonized overall nationwide or a national strategy for privacy rights in terms of the health sector.

Do you have any comments, or could you share your comments on this possible strategy?

Ms. Jennifer Stoddart: Yes, there is a strategy for harmonizing privacy principles and legislation across Canada, which is led by Health Canada, on which we've been consulted and in which we play a part. Yes, I would say certainly this is an ongoing concern as we move toward electronic health records.

Mr. Navdeep Bains: Correct. That's exactly it.

Ms. Jennifer Stoddart: You want to make sure that what's private in one jurisdiction is also private in another jurisdiction and you have information going from province to province in research areas and so on. It's a very important question. It's going to take some time to work through. My perception of the health field is that there are many actors—many institutional, professional, and governmental actors—but eventually we will harmonize either de facto or with something, possibly a legal framework, but I really can't speculate now to what extent that would be.

● (1700)

Mr. Navdeep Bains: Right now the discussion has taken place. The dialogue is there, right?

Ms. Jennifer Stoddart: Yes, Health Canada is leading a dialogue on which we are consulted. There is concern about PIPEDA, the intent of which I don't think is to regulate the health world per se. It only does it indirectly. At the time it was coming into force for all the general commercial sector and thus, by definition, doctors' offices and so on, we developed with Health Canada a series of 60 questions and answers. There is a reference from our website to their website for people across Canada. I was recently in Saskatchewan, where they have their own health legislation, which is slightly different, and I got comments that this was a really useful thing to have done. People like to go to our website and then be referred to the 60 questions and answers. I think we are going to work through this issue by discussion in the coming years.

Mr. Navdeep Bains: Has a timeline been set? Do we have an agenda, say, within one year or two years or three years that we plan to have a harmonized strategy? Is there a timeline in place?

Ms. Jennifer Stoddart: Not by my office, but it seems to me, from memory, Health Canada set a timeline of 2005. But it was some months ago that they mentioned this. I don't know whether that has been updated or how it is going.

Certainly, our office does everything possible in order to facilitate the voluntary emergence of shared common standards for privacy protection, so that we think dialogue with privacy partners in the public sector across Canada is very important.

The Chair: Time's up.

Mr. Hanger.

Mr. Art Hanger: Thank you.

I have two requests of your office, Commissioner. First, could you provide this committee with an organizational chart showing all positions and salary ranges? Second, could you provide this committee with a detailed breakdown as to what the funds in the estimate will cover?

Ms. Jennifer Stoddart: Yes, I could table that and send it to the clerk.

Mr. Art Hanger: Getting back to this concern between police agencies and private sector stakeholder investigative bodies, there's a definite issue dealing with the interpretation that hinders effective and efficient management of information sharing between these bodies. Often their legal counsel, I'm told...and it all centres around Bill C-6 and their belief of what an investigative body represents and what authority they have to share information under the right circumstances within the law. The one issue that has been brought to my attention is the apprehension on the part of police agencies to share an address—for instance, where a grow-op has been found—with a victimized private sector agency for fear of breaking privacy issues and opening them to possible liability and lawsuits for having shared what they feel is personal information.

I'm not going to get into all of this. But then they go back into common law torts as it may interfere with the investigative activities and the passing on of that information back and forth. To me this is a major issue. I'm surprised you haven't heard anything about it, given the fact that it does affect every law enforcement agency in the country and the investigative bodies associated with banks as well as insurance agencies. I would like some more clarification with regard to this interaction. I reflect back on your mandate as giving advice to both industry and public agencies.

Ms. Jennifer Stoddart: Could I suggest to the honourable member.... It's an important issue. It's a bit difficult for me to respond in the way you would like because I am trying to recollect a police association making representations to us about this recently. Could I get back to you? I don't know that there are any complaints here.

● (1705)

Mr. Art Hanger: There was a complaint in the sense that agencies will not pass information forward to one another, whether they're investigative bodies designated under the act or public police agencies, for fear of all of these civil repercussions. That is hampering investigations all over the country. I wish I could say I could divulge this information directly to you from the source from which I received it, but I don't want to, as I haven't had an opportunity to speak to them at length about doing that. When I have had, I will forward all the information to you, if that would be suitable.

Ms. Jennifer Stoddart: Yes, that would be very helpful. We could look at that and give a written response to your office.

Mr. Art Hanger: I would sure like that.

Ms. Jennifer Stoddart: That would be perhaps more useful. I'm sorry I can't answer your question, but we will do the research if you can send that to us and reply to you.

The Chair: I wish that your response, when you make it, would come through the clerk of the committee, because we're all listening and we're all interested and we'd like to know the answer.

Ms. Jennifer Stoddart: I see. Yes, certainly.

The Chair: Mr. Tilson.

Mr. David Tilson: I'd like to return to the topic of banking. One of the issues that have surfaced is the topic of identity theft. Considering that the banking industry is one of the largest collectors of personal information, perhaps second to the government, from all reports that I have seen, this problem is increasing. What can you do? What can the government do? What can the banking industry do to improve this?

Ms. Jennifer Stoddart: I think the police forces and the banking industry have a lot of specialized knowledge, so I'm not sure that I would—

Mr. David Tilson: All I'm saying, Ms. Stoddart, is that out of the blue people are saying, “Someone's doing things with my credit card”, or whatever. And you're right, the police are involved, but has this topic been discussed by your agency?

Ms. Jennifer Stoddart: The topic is discussed. We have periodic meetings with the representatives of the banking industry simply because privacy is so important to them. As we mentioned, there is a large number of complaints involving personal information in the hands of banks. Yes, we have discussed with them, generally, and I know they're very concerned about this and looking at ways of combating it.

I think the expertise of our office, though, is not in trying to tell the banks exactly, because of course they have information that we don't, about how they operate and where the fraud—

Mr. David Tilson: Except the problem seems to be coming from the banks. I'm saying this as a layperson. I haven't a clue, but my observation is, in looking at the reports, the problem seems to be coming from the banks because information is being released.

Ms. Jennifer Stoddart: I'm not sure this is the perception at our office, that the banks are responsible for identity theft. I think what you have is a new kind of criminality that has taken us unawares and that takes the combined efforts of many people. I think our office is most useful, in terms of its mandate and its expertise, in reminding the public about how to safeguard their personal information, and how to be wary, and how to take steps to prevent identity theft.

Mr. David Tilson: So when someone makes the complaint, do you say that's a police matter, or do you actually make an investigation?

Ms. Jennifer Stoddart: No. We can make an investigation if there's something we think we can usefully do. We could also encourage them to go to the police. But I think I'm trying to say to the honourable member that where we think we're most useful in the identity theft phenomenon is in reminding Canadians—and this comes back to some of the other comments I was making—of the importance of their personal information.

I think one of the issues is that because we've had a country with fairly high law enforcement standards and so on, people have been giving out a lot of personal information without thinking about it and how it can be used and misused. It's like crime prevention everywhere. I think this is where we're trying to focus on making our contribution to the issues of identity theft.

We're also in a Department of Industry task force that is looking at spam. Spam is a different problem from identity theft, but it's largely related in many ways. So we are collaborating in multi-pronged approaches to try to get at these kinds of phenomena.

● (1710)

The Chair: Time's up.

Mr. Hiebert.

Mr. Russ Hiebert: Thank you.

The Chair: Try to keep it fairly tight now, because we have a couple of motions we need to pass and we don't want to lose our members here.

Mr. Russ Hiebert: Yes. Don't start the clock yet.

I'm going to get my questions up front, and perhaps you can take note of them and respond so I don't lose any more time.

We've talked a lot about border issues and about sharing information with the United States. My questions are very straightforward. Specifically, what personal details are gathered at our border crossings? Is any of this information shared with U.S. officials? If so, what potential harm do you see in sharing some or all of these details, such as mundane travel details, residence information, with officials on the other side of the border?

Ms. Jennifer Stoddart: So the first one, then, is what are the details?

Mr. Russ Hiebert: What information is there, is it shared, and what are the concerns with sharing it if it is?

Ms. Jennifer Stoddart: Exactly what details are shared now at border crossings is exactly the objective of the audit that we hope to carry out this year. I think your question reflects the concerns of many Canadians, and we would like to be able to say that to them, but I cannot answer the question right now.

Your second question is...?

Mr. Russ Hiebert: Is it being shared?

Ms. Jennifer Stoddart: Yes, we understand it's being shared through previous audits that we have done on various agencies that work in border exchanges. Yes, there is sharing of information with the United States at the present time.

Mr. Russ Hiebert: The third question is, then, are there any concerns about sharing this information?

Ms. Jennifer Stoddart: Yes, there are concerns. Some of them we have mentioned in our annual report. We're concerned that the controls on sharing the information are not as tight as they could be.

Mr. Russ Hiebert: All right.

Do I have time for a supplementary?

The Chair: Very quickly.

Mr. Russ Hiebert: Very quickly.

Canadians seem to be raising all kinds of actions as offending the Privacy Act. I was recently informed about somebody who said that they are no longer to give out name tags because it offends the Privacy Act. So people are obviously taking this to an extreme. I'm wondering, what efforts at public education is the commission taking to sensitize Canadians to the fact that this is not a police state we're living in? People are still free to share information. I think the pendulum is going way too far.

Mr. Raymond D'Aoust: We are certainly taking steps through mainly our website and also meeting with business associations and so on to clearly convey the fair information practices, if you will, or principles that are enshrined in the PIPEDA legislation. So it's mostly through our public information and public education material that we attempt to do that. The commissioner certainly has met with a number of those groups since he joined the office, so we are making efforts to dispel some of those myths.

Mr. Russ Hiebert: That's certainly needed, I think. Thank you.

The Chair: Great, thanks.

Mr. Broadbent.

Hon. Ed Broadbent: Yes, I have two short questions.

First, if I understood you correctly before on the issue of the CIBC Visa problem vis-à-vis the Patriot Act in the U.S. having the effect of Visa holders' private information being passed on to the U.S. simply because CIBC is using a U.S. processor.... If I understood your reply, I take it that the PIPEDA legislation as it now exists is insufficient to deal with that problem, because you said to me that we could bring in legislation that would deal with it.

Ms. Jennifer Stoddart: The PIPEDA legislation does not prevent the outsourcing of work, including Canadian's personal information, abroad. What it does do, though, is say that the person who holds the data, who is accountable for it, must ensure that the other entity to whom this information is given treats it in accordance with Canadian standards. That is not, however, necessarily a shield against the application of the American Patriot Act on American territory.

● (1715)

Hon. Ed Broadbent: The other person who gets the information in the U.S. has to use it according to Canadian standards?

Ms. Jennifer Stoddart: That's right. That means apply by the principles of PIPEDA, which are the fair information principles in terms of confidentiality, access, not passing it on without consent, etc.

Hon. Ed Broadbent: So I understand the security, this information that goes to the U.S. about Canadians, personal information, goes to the U.S., and we're saying that because it's going from us, the U.S. use of this has to comply with our standards, which would imply extraterritoriality, the application of—

Ms. Jennifer Stoddart: I think it's a version of that. We obviously cannot regulate what happens in the United States. We're saying the entity that passed it on to another one, whether it be in Canada or out of Canada, is responsible within Canada to the person who gave them that information. That is what Canada has legal authority over, you see. We hold the Canadian entity responsible for how it passes information on, but we cannot technically regulate what is happening to that information in a third country. So your recourse would be against the Canadian-based entity that passed it on elsewhere.

Hon. Ed Broadbent: Wouldn't it be simpler just to stop it from passing it on?

Ms. Jennifer Stoddart: Certainly if you didn't want it to be transferred from Canada to other countries, yes, it would be simpler.

Hon. Ed Broadbent: I'm really trying to understand this, because if it got into the hands of U.S. security forces or whatever—and that's not criticizing them for looking after their own interests, but I am concerned that if they look after their own interests by impinging upon the privacy of Canadians.... If this gets into the hands of U.S. security forces, who don't have the best record in recent history of treating people in an outstanding way, with the CIBC as a transmission agency, how do we control in any way, once it leaves our borders, how it's dealt with in the U.S.?

Ms. Jennifer Stoddart: I don't think we can.

Hon. Ed Broadbent: But we can stop it, can't we, if we have a law?

Ms. Jennifer Stoddart: If Parliament passed a law that said we do not outsource Canadians' personal information to any other country, it would be stopped.

Hon. Ed Broadbent: According to the last question, according to what Mr. Alcock said in the House of Commons, after meeting with you, he was assured that with the PIPEDA legislation we have all the authority we need to ensure that these incursions do not take place—that is to say, the transmission of private information.

Did you offer him that assurance, that we have all the authority in existing law?

Ms. Jennifer Stoddart: I explained to him the functioning of PIPEDA the way I am explaining it to you now. That is the only position our office takes. It's explained in more great detail in the submission to the B.C. commissioner, which is on our website.

I don't think any country regulates, really, the use of information outside its own borders, but to the extent we can, we do have a law that says any information sent out of Canada has to be sent out according to the standards, if the organization falls under PIPEDA, that PIPEDA sets out.

Hon. Ed Broadbent: Thank you.

The Chair: Time's up.

Our last questioner is Mr. Laframboise.

[*Translation*]

Mr. Mario Laframboise: Thank you, Mr. Chairman.

As regards personal information, I see that 55% of the complaints received and 80% of complaints handled come from the Correctional Service of Canada. What's the problem with the Correctional Service of Canada?

Mr. Raymond D'Aoust: We provide some details on that subject on page 26. A number of those complaints came from employees who said they had been denied access to their personal files. We investigated one complaint of that kind, which was a multiple complaint. We also received complaints from inmates who said their personal information had been wrongly shared, etc.

● (1720)

Mr. Mario Laframboise: I see that the majority of complaints come from British Columbia, Alberta and Quebec. Do most of those complaints come from the Correctional Service of Canada in those provinces?

Mr. Raymond D'Aoust: Yes.

[*English*]

The Chair: Thank you.

I thank you for your excellent answers and for your time. As you can see, the committee is feeling its way around these issues. It looks as though we have lots of interest to get into some studies on some of these issues once we're finished with these estimates.

Thank you very much for coming. We look forward to having you back again reasonably soon.

Ms. Jennifer Stoddart: Thank you very much for welcoming us, and thank you for your very thoughtful, challenging questions. We will be back. I think we have tentatively scheduled December 1 for that.

The Chair: We have to talk to the committee about it and make that decision.

Ms. Jennifer Stoddart: Okay. And we'll work on the requests for information that you've given us.

Thank you very much.

The Chair: Colleagues, I'd like to ask you to vote on these estimates so that we can report them back to the House, if we may. After that, we need to decide on future business, and we have the supplementary estimates of the Privacy Commissioner to deal with. As you just heard, we have a suggested date for that, but it will be up to you.

First let's deal with today's votes.

Justice

Ministry Summary

Offices of the Information and Privacy Commissionersof Canada

Office of the Privacy Commissioner of Canada Program

Vote 45—Program expenditures.....$3,918,000

Office of the Information Commissioner of Canada Program

Vote 40—Program expenditures.....$4,443,000

(Votes 45 and 40 agreed to)

The Chair: Shall I report the votes to the House?

Some hon. members: Agreed.

The Chair: Thank you, colleagues.

We have a suggestion for a subcommittee on future business for Monday, November 29. Check your calendars and see if that will work for you.

Mr. Derek Lee: For you, my Mondays are always free.

The Chair: Okay.

We have to report the supplementary estimates for the Privacy Commissioner on or about December 6, so we have to deal with them fairly quickly. We have a suggested date of Wednesday, December 1.

Mr. Derek Lee: Can I ask, the supplementary estimates, is that the PIPEDA? We just walked through that today.

Do members want to go through the whole thing again with...? Yes? Okay.

Mr. Hanger has some robust questions.

The Chair: So the date is okay, December 1? We've set that up?

I guess, Mr. Broadbent, if there's a problem we'll contact your office to see if Monday, November 29, will work for you and Monsieur Laframboise.

The other thing I wanted to mention before we adjourn is that it has become pretty obvious to me that three minutes is not enough time to get a thought across. So with your permission, I'd like to go to five minutes on those rounds, if we could.

Most of you got five minutes today, anyway.

Mr. Derek Lee: Could I talk to that?

The three-minute round is meant to allow all the members to participate. We got along pretty well today and it worked fairly well. But if we go to five minutes, the five will become six, seven—that's my experience.

The existence of a three certainly allows the chair two and a half minutes to indicate to the questioner that he or she's near the end. With the discretion of the chair, the three, I think, is reasonable. But if we go to five, your hands, Mr. Chairman, will be tied at Mr. Lee going on a five-minute diatribe and not getting to a question.

● (1725)

The Chair: All right.

We'll continue with that, then, if you'll give me a little discretion on it, because I'd like to allow the witness to complete a thought.

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 Parliamentary Internet Parlementaire at the following address:
Aussi disponible sur le réseau électronique « Parliamentary Internet Parlementaire » à l'adresse suivante :
http://www.parl.gc.ca
