House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 004 • 2nd SESSION • 40th PARLIAMENT

EVIDENCE

Monday, February 23, 2009

Chair

Mr. Paul Szabo

Standing Committee on Access to Information, Privacy and Ethics

Monday, February 23, 2009

● (1535)

[*English*]

The Chair (Mr. Paul Szabo (Mississauga South, Lib.)): Good afternoon, colleagues. This is the fourth meeting of the Standing Committee on Access to Information, Privacy and Ethics. The order of the day, pursuant to Standing Order 108(2), is a briefing from the Office of the Privacy Commissioner.

Today we have with us the Privacy Commissioner, Ms. Jennifer Stoddart. Welcome back to our committee. I understand that you have an opening statement to make, but you may want to start by introducing the colleagues you brought with you.

Yes, Mr. Poilievre.

Mr. Pierre Poilievre (Nepean—Carleton, CPC): Mr. Chair, I don't like to interrupt, but I was wondering if it would be possible, given the public interest in the subjects we'll henceforth be discussing today, to open the discussions to televised hearings.

The Chair: Are there any comments from the members? It's something the committee would normally request in advance so as to make those necessary arrangements.

Go ahead, Madame Freeman.

[*Translation*]

Mrs. Carole Freeman (Châteauguay—Saint-Constant, BQ): Mr. Chairman, if we had wanted this to be televised—

Mr. Pierre Poilievre: It isn't hard to start up the cameras. They're already here.

[*English*]

The Chair: Thank you.

I understand that it would take some time to do it. We could technically do it, but I'm not sure, at this point, that the committee seems to reflect an enthusiasm for doing it or for taking our time for that now. So why don't we proceed?

Madam Stoddart, please introduce your colleagues, and let's proceed with your presentation.

Ms. Jennifer Stoddart (Privacy Commissioner, Office of the Privacy Commissioner of Canada): Thank you very much, Mr. Chairman.

It's a pleasure to be here again with the committee, our committee. As an agent of Parliament, we report to you.

With me today is Chantal Bernier, who's just joined us as assistant commissioner for the Privacy Act. You may remember

[*Translation*]

Raymond D'Aoust, who was assistant commissioner. His term ended in September and he was replaced by Ms. Bernier.

[*English*]

Also with me today is Lisa Campbell. I believe you met Lisa Campbell, our acting general counsel. She came up last week. Unfortunately, I had another engagement, briefing a minister, I think, on our upcoming report. She came with Mr. Tom Pulcine, who is just behind me and whom you'll recognize. Also here with me today are two other members of my staff: Éric Charlebois, who is our parliamentary liaison officer, and Ann Goldsmith, who's head of the policy section.

I'd also like to say, Mr. Chairman, that Elizabeth Denham, who is the commissioner for PIPEDA,

[*Translation*]

the Personal Information Protection and Electronic Documents Act,

[*English*]

is in Calgary this week and unfortunately can't be with us.

Members, Mr. Chairman, you can see that we've supplied you with a fairly thick binder of information about the Office of the Privacy Commissioner, about our statutory responsibilities, and about some of the issues currently preoccupying us, and we hope that you'll find it a useful reference.

As Privacy Commissioner, for those of you who aren't too familiar with what I do, I'm an independent officer of Parliament. I report to Parliament, which means through this committee, through annual reports, or through special reports.

My office, with its 160 employees, is responsible for overseeing two laws: the Privacy Act, which covers federal departments and agencies—this has just been increased through the Federal Accountability Act—and PIPEDA, which is short for the Personal Information Protection and Electronic Documents Act. PIPEDA, which was adopted almost 20 years after the Privacy Act, covers private sector organizations, including retailers, financial institutions, airlines, communication companies, and so on.

The objective of both these laws is to protect the privacy of Canadians by setting out the ground rules for how organizations collect, use, and handle personal information.

[*Translation*]

I'm going to continue by talking about privacy threats. I would be happy to elaborate later on the philosophical underpinnings of these laws, but suffice it to say that there has never been a greater need for them.

The threats to the privacy of Canadians are real and they are grave. For my Office, a major challenge is the fact that the list of issues we must address is long—and growing longer every day.

Technology, for all its benefits, has created unprecedented threats to privacy. I'm thinking here of surveillance technologies, electronic tracking devices, and biometric scans, among others.

Computer memory has never before been so plentiful and cheap, which makes it incredibly easy, not only to compile information about people, but also to cross-reference it, manipulate it, analyze it, massage it and sell it to the highest bidder.

Many businesses now see detailed personal information as essential to their marketing efforts. Governments are increasingly interested in personal information as part of their national security efforts.

And in recent years there has also been a growing recognition by thieves that they can make a lot of money by stealing names, birth dates, credit cards and other personal information. According to the RCMP, organized crime groups in Canada now see personal information as an important money-maker that complements their more traditional sources of income.

● (1540)

[*English*]

Many of the emerging risks for privacy involve incredibly complex technologies. My office needs to delve into highly technical matters, such as nanotechnologies, genetic technologies, and deep-packet inspection techniques, to name just a few examples.

Later this week my office is appearing before the public safety and national security committee on the review of the DNA Identification Act.

Adding to the complexity is the fact that many privacy issues are now global in nature. “Cloud computing” has entered our vocabulary. Data flashes around the planet literally at the speed of light, which challenges us to ensure that the personal information of Canadians is protected on the other side of the world.

Whatever we do within our borders will never be enough to protect Canadians' privacy abroad. So we work with other countries to develop a basic level of level of data protection around the world. To this end, my office has been a keen participant in a number of international privacy initiatives by the Organisation for Economic Co-operation and Development, or OECD, Asia-Pacific Economic Cooperation, or APEC, and other organizations.

[*Translation*]

Now I'll move on to the issue of legislative reform.

On the legislative front, you will recall that I appeared before this committee last year to talk about the mandatory review of PIPEDA. I am pleased to report that the process is continuing apace, and I look forward to amended legislation coming forward through Industry Canada in the near future.

I would also like to mention another significant challenge for my Office—the Privacy Act.

As I—and a string of privacy commissioners before me—have pointed out to parliamentarians over the years, this piece of legislation is seriously outdated and in urgent need of reform. To add a bit of perspective, consider this: when that law was passed, the Commodore 64 was a novelty.

Last spring, this committee launched an important review of the Privacy Act. I presented a list of 10 quick fixes that would bring some immediate relief. But, in the long run, the legislation needs a complete overall to bring it in line with the privacy challenges of the 21st century.

I know the committee has heard from many witnesses and I look forward to responding to their comments and speaking further on this issue with you.

[*English*]

In conclusion, reforms to Canada's privacy laws will have to start here, in this committee, with you. I would suggest to the honourable members of this committee that privacy is an issue that should be of concern to all Canadians, regardless of political beliefs.

The threats to privacy that confront Canadians may not always be apparent to the average citizen. Indeed, the risks are often subtle and nuanced. They don't tend to appear all at once, but rather in a stealthy and gradual manner and from many different directions.

Canadians cannot possibly defend themselves against such threats alone. They need a government that sees privacy as a human right and that sees personal information as a commercial asset that must be valued and properly protected.

As an officer of Parliament, my job is to support you in this important role. My office is currently developing materials for householders, such as information on identity theft, to help you talk to your constituents about privacy.

We look forward to working closely with you to ensure that the privacy rights of Canadians are protected, and I welcome your questions.

● (1545)

The Chair: Thank you kindly.

You are probably aware that the committee has already discussed and agreed to complete the work on the study that we conducted. I think the only other thing before we get too far into that—and you may have already given this some consideration, but if not, I would appreciate it if you would—is if you think there are any other witnesses you believe this committee should meet. We have a draft report coming, but that doesn't mean we can't continue to top it up to ensure that the dialogue that we had is fairly reflective of the attitude out there in the privacy legislative sector. So I invite you to do that.

Ms. Jennifer Stoddart: Thank you.

The Chair: The other aspect of this, which you haven't commented on, but which I guess we'll get into, and on which maybe you could start your mind whirling, has to do with the human resources issue. As you know, the committee expressed some significant interest and concern about the ability of the commission to discharge its responsibilities. It came out in the review of the legislation and in some of the recommendations or possibilities that were posed to us for improvements in the act.

But separate and apart from that, I believe that we were asking for —and Mr. Hiebert may recall this—updates or progress on the human resource initiatives and backlog issues, so that we could continue to monitor these responsibly and, if necessary, become more involved. It is a situation that exists not only in your own commission, but also, as you know, even in the Office of the Information Commission, and I suspect maybe in other areas too. This may be something that we would have to take up possibly with the Treasury Board, or another jurisdiction, to find out how we can facilitate relief of a very serious situation where you don't have the manpower to discharge your responsibilities. It comes down to that, very simply.

Anyway, so much for my comments. I'd like to be begin our first round with Mr. Wrzesnewskyj, for seven minutes.

Mr. Borys Wrzesnewskyj (Etobicoke Centre, Lib.): Thank you, Chair.

Commissioner, welcome.

I noted that in your reports the majority of complaints are about the RCMP. When you went through those complaints, approximately what percentage were valid complaints?

Ms. Jennifer Stoddart: We do publish a quite extensive cross-tabulation in our annual report.

While my colleague looks for that, perhaps I could say that, generally speaking, relatively few of the complaints are founded under the Privacy Act. It's only a minority of complaints that are founded under that act, which I guess is good news in terms of the privacy practices of most of the organizations. Some are settled in the course of the investigation.

We could give you that information later.

Mr. Borys Wrzesnewskyj: While it's being looked up, which particular departments within the RCMP do most of the complaints stem from?

Ms. Jennifer Stoddart: I don't know, Mr. Chairman, that I've seen that specific figure or that we've analyzed it.

That's quite an interesting question.

Mr. Borys Wrzesnewskyj: If that information could be—

The Chair: To the extent that we get into areas where it's a little detailed and you're not prepared to fully answer the questions with 100% confidence, I would suggest that you take the question and undertake to respond.

Ms. Jennifer Stoddart: I'll take it under advisement, yes.

Mr. Borys Wrzesnewskyj: Okay, perfect. Thank you.

Are you aware of valid complaints stemming from ATIP requests that were released and ended up causing embarrassment, etc., in regard to people's privacy?

Ms. Jennifer Stoddart: I believe that we do have a few of those a year, but they're a rather rare occurrence, because the releasing department in these cases relies on the public interest override, if it is an issue of community safety or the general public needs to know something about it.

So it's discretionary. Even if somebody does complain, it's up to the department head.

● (1550)

Mr. Borys Wrzesnewskyj: So there have been complaints in the past. Like you said, there may have been community overrides and perhaps community safety issues at stake.

Have you ever come across a situation where a briefing note to the commissioner was released, a briefing note that touches upon a potential criminal investigation into the actions of a member of Parliament? One would assume, this being a briefing note from the commissioner, that immediately within the ATIP section it would cause people to be especially mindful and careful of how they proceed, combined with the fact that it touches on a member of Parliament and a member of Parliament's reputation.

Is it not quite unusual that an ATIP document would be released—in this case the briefing note to the commissioner—which would in fact identify one of the individuals, a potential individual in a criminal case that went nowhere? Mr. Bill Casey was identified in this document that was released publicly. Has anything as serious as this happened in the past with the ATIP section in any of the complaints you've seen?

Ms. Jennifer Stoddart: We have not done an analysis of particular issues such as briefing notes being released. As I say, the department heads do have wide discretion under the Privacy Act to release personal information exceptionally when they believe there is a public interest. We'll have to leave it at that.

Mr. Borys Wrzesnewskyj: I noted in one of the reports in our binder here what your office audit found about the RCMP gathering information. I'll actually quote it. They used a phrase to say that the RCMP was gathering information "in excess of what is allowed or required". Was that information just beyond the scope of what's allowed or required? Was any of that information illegally obtained?

Ms. Jennifer Stoddart: Could I ask, Mr. Chairman, if the honourable member is referring to our special report on the exempt banks?

Mr. Borys Wrzesnewskyj: I believe it was your special report to Parliament in February of 2008.

Ms. Jennifer Stoddart: Yes.

Mr. Chairman, we did not study the question as to whether the information had been obtained illegally. That is not within our mandate. We just looked at the information and its relationship to the administration of the Privacy Act.

Mr. Borys Wrzesnewskyj: Okay.

I understand that the RCMP has a number of exempt databases, so they're exempt from your ability to look into them and they're exempt from these privacy regulations. How many such databases are you aware of besides Project Shock?

Ms. Jennifer Stoddart: If I may just add to the comment of the honourable member, "exempt banks" doesn't mean they're exempt from us looking at them. That is how we did the report on the exempt banks. That kind of report hadn't been done for a while. It means that the ordinary member of the Canadian public finds that these banks are exempt from their right to access their own personal information for national security reasons. That's how they're exempt.

Mr. Borys Wrzesnewskyj: Okay. So how many are there?

Ms. Jennifer Stoddart: As far as I know, now there's only one.

Mr. Borys Wrzesnewskyj: Is it Project Shock?

Ms. Jennifer Stoddart: No. Project Shock was closed. The Project Shock exempt bank was closed as a result of our audit.

Mr. Borys Wrzesnewskyj: I see.

The Chair: You have half a minute.

Mr. Borys Wrzesnewskyj: How many people would have been on that data bank, Project Shock, and on the current one that's still functioning?

Ms. Jennifer Stoddart: I'd have to get back to you on the exact number.

Mr. Borys Wrzesnewskyj: Yes, and this—

The Chair: We're there, Mr. Wrzesnewskyj. Thank you.

Mr. Borys Wrzesnewskyj: Thank you.

The Chair: We're going to move on to Madam Freeman now.

[*Translation*]

Mrs. Carole Freeman: Good afternoon, Ms. Stoddart, Ms. Campbell and Ms. Bernier. Thank you for being here today.

I entirely agree with you that this act is completely obsolete, since it dates back 25 years. With 25-year-old tools, it therefore cannot address today's technological issues.

I carefully read the 10 recommendations you referred to. I also noted that you had set priorities. Among the four priorities you want to address in the policy and research areas, I see emerging information technologies. Can you further explain the kind of work you intend to do in this regard and in the areas of identity and national security?

● (1555)

Ms. Jennifer Stoddart: Mr. Chairman, I would like to ask my colleague Ms. Bernier to respond to the member on that subject, since she is supervising the work on priorities.

Ms. Chantal Bernier (Privacy Commissioner , Assitant Privacy Commissioner): Indeed, I've been asked to coordinate the four priority projects, each of which is directed by one person. Simply to give you some background, I'll say that these projects concern respectively technology, developments in genetics, developments in national security policy and identity management.

To answer your question, then, I'm going to tell you about what we're doing specifically with regard to technology. As you'll no doubt understand—the Commissioner moreover said this in her opening remarks— we must be at the forefront of technology and we must very carefully monitor developments with respect to privacy.

What we're doing can be divided into four major components. The first consists in forming the greatest understanding and the greatest possible expertise in technology so that we can truly understand the scope, extent and impact of the various technologies. So we're working on research and training projects on identity systems, technologies such as RFID and on biometrics, for example.

We're also taking part in international work in order to genuinely take advantage of information sharing. In our audits, we're focusing particularly on certain types of communications such as wireless communications. We're also starting an audit at six departments that were selected on the basis of our analytical work to see how wireless communications are managed.

In short, the purpose of our activities is, on the one hand, to develop and broaden our expertise and, on the other hand, to see how federal institutions manage the information retained through technology in order to protect privacy. In this area, I am responsible for the Privacy Act.

Mrs. Carole Freeman: So you're trying to stay at the forefront of emerging information technologies.

I saw the organization chart of people working on your team. You have a titanic job.

Only yesterday, on the program *Enquête*, there was a report on the virtually childlike ease with which computer hackers can, in the space of five minutes, recover information such as names, addresses and telephone numbers from our departments.

You're no doubt familiar with Mafiaboy, that young man of 15 who completely paralyzed all the Internet search engines. This is all the more disturbing since the incident I'm referring to dates back a few years.

What have you done since then to protect the identity of people in our federal organizations?

Ms. Chantal Bernier: We're doing a lot of things. First, we're conducting assessments of the impact certain programs have on privacy, in cooperation with the federal institutions. When they introduce a program that can leave room for an invasion of privacy, they conduct an assessment of it.

For example, one of those ongoing assessments received some media coverage. It was the Canadian Air Transport Security Authority pilot project in Kelowna, in which they used what's called the Integrated Checkpoint System, a machine for viewing passengers with the aid of holographic images. That was reported in the press. The Administration got us involved in it from the outset. We haven't issued a decision or judgment, but we're working with the administration's representatives to assess the impact on privacy.

So this is an upstream job to determine in advance whether a proposed program would be consistent with privacy. That's one of our activities.

We're also proceeding with audit activities. Once a program is in place, we determine whether personal information management is adequate. We also do policy development work, research work and public information work.

With respect to technology, I'll give you a recent example. Two weeks ago, we handed out some awards for videos produced by young people in which they had to show how technology can compromise personal information. It was a contest held in Canada's high schools. Projects were submitted, and we awarded prizes for the best ones. That was one way of making youths aware of the dangers of technology.

There are a host of examples, even though I've just given you a few.

● (1600)

Mrs. Carole Freeman: What you say is very interesting, Ms. Bernier. On the other hand, the purpose of my question was to determine how you go about protecting personal information that departments and agencies have on citizens.

We know that computer hackers can very easily hack into the systems of federal organizations to recover data. Yesterday on Radio-Canada, *Enquête* very clearly explained over the one-hour program how easy it is to access organizational data bases directly.

[*English*]

The Chair: Merci, Madame.

[*Translation*]

Ms. Jennifer Stoddart: Mr. Chairman, I'm going to supplement my colleague's comments.

For a number of years now, we have urged the Government of Canada to adopt a cyber security policy. We clearly have to have such a policy. I believe that Canada is now one of the only OECD countries without a policy on its cyber infrastructure. That's quite serious.

I would like to point out to you that our office does not have an obligation to protect data. That's up to each department, agency and organization. However, we increasingly take the opportunity to remind them of their responsibility in both the private and public sectors. The two acts, that is to say the Privacy Act and PIPEDA, require that all data be protected from all threats so that it remains confidential. Where there is an attack, we can investigate and suggest remedies. We've done that in a number of cases.

[*English*]

The Chair: Thank you.

Mr. Siksay, go ahead, please.

Mr. Bill Siksay (Burnaby—Douglas, NDP): Thank you, Chair.

Thank you for being here, Ms. Stoddart.

It's good to see you again, Ms. Campbell.

Congratulations on the new job, Madame Bernier.

My question, Ms. Stoddart, is about security for the Olympics. I know earlier this month you were in British Columbia to participate in a workshop on security for the Olympics. You raised a number of concerns that you had about the Olympics and security, particularly security post-Olympics. I wonder if you might share with us some of the concerns you raised at that time.

Ms. Jennifer Stoddart: Once again I would ask that my colleague Madame Bernier answer this, since before joining our office—as you probably read—she was assistant deputy minister of public safety. She has a great knowledge of security issues, which means that she was immediately assigned this file. In fact she met with the RCMP in Vancouver, so she can give you a much better description of it than I can, if you would allow that, Mr. Chairman.

[*Translation*]

Ms. Chantal Bernier: Of course.

[*English*]

We have a series of concerns, but they are not concrete in the sense that we have observed some practices that are of concrete preoccupation. However, the question arises obviously from having an intensification of security, which leads to an intensification of the duty to protect privacy. I had a list of questions that I shared with the RCMP in advance of our meeting, which was on February 5. The RCMP met with us for three hours and answered all of our questions.

We asked the RCMP if they have a policy specifically for that occasion, being so exceptional, to protect privacy within the security measures they have to take. Secondly, will they train their officers? Will they ensure that the security, and therefore any intrusion into someone's privacy, not become the norm?

We will also ask them to make sure that any foreign governments will not have access to information they should not have access to. So how are they protecting Canadians' current rights to privacy within this exceptional context?

Their answer, in fact, was much more detailed, but you can see a summary in their own press release of February 4, which was very much based on the questions we had put to them.

● (1605)

Mr. Bill Siksay: Can you share a bit about that? I know that in this kind of large-scale event there are provisions for security that are sort of unusual and extraordinary that would go to the concerns about privacy. Can you raise some of the specific issues you might have raised or that might come to mind, given this kind of event?

Ms. Chantal Bernier: On the question of how they were going to manage the information, they said they would ensure that current Canadian laws would be fully, rigorously respected. Their general counsel was there and said that he assumes that responsibility.

In relation to surveillance itself, it will not go beyond what is strictly necessary. For example, one of the concerns we had was the possible overuse of closed-circuit cameras. They said they would be minimal and would be used exclusively as necessary and would be turned mostly towards prohibited zones. Hence, if a person were captured on one of those cameras, it would be because he or she had in fact trespassed. There will be, of course, cameras outside. The RCMP is in a much better place than I am to answer that, but they were saying they would make every effort to be compliant globally. We are engaged with them in a continuing dialogue on that.

Mr. Bill Siksay: One of the issues Ms. Stoddart raised in the media was the dissembling of some of these security arrangements post-Olympics, whether the same level of security would just fall into the hands of law enforcement and be used on an ongoing basis. Was there a response specifically to that concern?

Ms. Chantal Bernier: They said that the equipment would be on a lease service contract. They would not retain any of the equipment, and therefore they did not feel that this was an issue, that they would not keep the equipment.

Mr. Bill Siksay: So the RCMP won't keep it, but somebody else may have it on a leased basis?

Ms. Chantal Bernier: They said that they will not keep it. They said that it would be a lease contract, a service contract, and that therefore past the need—the actual Olympics—they would not have that equipment any more.

Mr. Bill Siksay: You don't have any sense about whether that security infrastructure would be disassembled and returned to a more normal sense of security at some of those venues or in those communities?

Ms. Chantal Bernier: I can tell you the sense that they gave us is that there would not be a legacy of increased security beyond the need occasioned by the Olympics.

Mr. Bill Siksay: Do you know if there is any provision in the budget for security at the Olympics to do any of that kind of removal or disassembling of the security infrastructure?

Ms. Chantal Bernier: I don't know. I have not seen their budget.

Mr. Bill Siksay: Okay.

The whole issue of closed-circuit television surveillance is one. I know Britain has gotten into it very heavily. The United States seems to have adopted it. Do we have any estimation of how much it's used in Canada in comparison with those other countries?

Ms. Chantal Bernier: We've actually funded a research project by Queen's University. I've read the draft report. It's being finalized. It will be released, I understand, before the end of March. So if you want, we would be happy to send you a copy. Obviously it's for dissemination.

Mr. Bill Siksay: That would be great.

Do you know if there was any increased video surveillance or infrastructure installed in Ottawa during President Obama's visit, and were there any concerns that came out of that?

Ms. Chantal Bernier: I have no idea.

Mr. Bill Siksay: Another issue that you raised in your report and that impinges on British Columbia is the whole enhanced driver's licence project. And I know that's coming up. Actually my driver's licence is due to be renewed in March, and I did check with them and found out that the enhanced licences are available starting the second of March, I believe, in B.C. I'm just wondering where your concerns are at with that project at this point. I know it's one you've been following.

The Chair: Madam Stoddart.

Ms. Jennifer Stoddart: Our concerns are very much those of our colleague, B.C. Information and Privacy Commissioner Loukidelis. In fact, we're working together with him and with a number of other provincial commissioners on that. We're concerned at various levels. We continue to be concerned about access to the information. When a Canadian crosses the border, how much information is transferred with him or her? We have concerns about the technology and the extent to which the information can be captured by those other than border service agents. We are concerned about the extent of background checks that go into the issuing of one of these enhanced driver's licences, about how this links into other security issues that we may not know about.

So we're certainly watching this with great interest. We've made some suggestions to the Canadian government in our response on a privacy impact assessment, and we continue to talk about this on an ongoing basis, as the results of the trial will come in soon.

● (1610)

The Chair: Thank you.

Mrs. Block, please.

Mrs. Kelly Block (Saskatoon—Rosetown—Biggar, CPC): Thank you very much, Mr. Chair.

I want to take it back to some of the comments that Ms. Freeman had made, or questions that she'd asked. You made the comment that it is not your job to protect the information but to ensure that different organizations are complying with legislation. A few months ago I would have considered myself an average Canadian. If average Canadians knew what you knew about privacy laws and how they are being enforced to protect Canadians, do you think they would be satisfied with how their privacy is being protected? And based on your answer, could you give us some examples of why or why not?

Ms. Jennifer Stoddart: I in fact get a lot of information from the same sources as other Canadians. I may just get specialized information a little sooner from some of the studies that we do. We know that Canadians are very concerned about how their personal information is handled. They're concerned about security. They're concerned about transborder data flows, that information may go to a country that has lower data standards and so on. So that's a constant theme that comes up again and again.

Could you just repeat the second part of your question?

Mrs. Kelly Block: Do you think Canadians would be satisfied with how their privacy is being protected right now, here in Canada, based on whether they know what you know?

Ms. Jennifer Stoddart: No, I think with what they know now, they're concerned and they're not satisfied with how their personal information is protected. One indicator of that is the tremendous interest in recent years in the work of my office, both in the public and the private sector.

Parents are worried about their children's privacy because the children spend all their time online now. We've got eight million Canadians on Facebook, and it's not clear where their information is going once it's on Facebook. That's one of our ongoing investigations. People are worried about their personal information being stolen. ID theft is rampant, unfortunately. I've mentioned ID theft issues before this committee in the past and have ongoing recommendations that we amend the Criminal Code and that we pass anti-spam legislation.

Canadians who can't afford expensive software updating packages are exposed to a lot of spam. Just on my government computer, I'm told that 98% or 99% of the e-mail we get is spam. The Government of Canada can afford pretty sophisticated spam filters, but it shows you the extent of the global problem. We're the only one of the G-8 countries that has no anti-spam legislation.

So I think Canadians are pretty realistic that they don't have all the privacy protection they need.

Mrs. Kelly Block: Thank you.

I have a follow-up question based on the report we received. Do you travel to other countries in your role as Privacy Commissioner?

Ms. Jennifer Stoddart: Yes, I do.

Mrs. Kelly Block: Can you tell us some of the events and/or conferences you have attended in your role in the past 12 months?

Ms. Jennifer Stoddart: Yes. Let me try to think of this in reverse order.

In October I travelled to Strasbourg with members of my office to take part in the International Conference of Data Protection and Privacy Commissioners. We had hosted the event in Montreal a year before and had been invited by members of the committee. That conference was opened by the Speaker, Mr. Milliken, which was an honour for us and a link with our parliamentary function. We go to that every year.

Prior to that, outside the country I was with the ministerial delegation of Industry Canada in Seoul, South Korea, in the context of OECD work, where my office has been very active in drawing up cross-border procedures for the sharing of remedies in cases of mismanagement of personal information. I participated on a panel and was part of the discussion among the Canadian delegation.

Prior to that, I was in London giving a speech to an international e-crime conference about the lessons that could be learned from the joint investigation between my office and the office of the Information and Privacy Commissioner of Alberta on the TJX affair, which had to do with hacking into a TJX database and stealing some million credit cards. This had repercussions worldwide. The people are just being brought to justice, but millions of dollars in damages were paid out.

Prior to that, I was at the OECD for a working meeting. I think that's back to last March.

Does that give you an idea of what takes me out of the country?

● (1615)

Mrs. Kelly Block: Yes, absolutely.

From reading your report and hearing what you're saying, it would appear you have played a lead role in some of the conferences you've attended. Can you tell me what you have learned at these conferences? And how do Canadian privacy laws compare with privacy laws in these other countries you have had the good fortune to visit?

Ms. Jennifer Stoddart: There are two main things. One is that the Canadian approach is of great appeal. The privacy world is divided into three groups: people who don't have privacy legislation, then there are people who take an approach like the European Union does, and then the approach of the United States, which doesn't have overall privacy legislation. The Canadian version of this blends in both the European and the American approaches. So it's of great interest and great appeal because it adapts itself to many situations and many cultures.

However, that's the good thing. The sometimes depressing thing is the rate to which Canada has fallen behind in its privacy protection and the extent to which we are challenged in enforcing some basic measures. One honourable member raised the question of security. We have no data breach notification legislation, unlike that in most states. We do not have a system that really deters to any extent a lot of misdoing. Within our own government we have a very opaque system of management of personal information that needs to be seriously looked at. The average Canadian has no recourse. If the federal government misuses his or her information, there really is no recourse. You just have a right to get access to your information, but if they've misused your information and made some egregious mistake that causes you harm, as is the case of Mr. Murdoch from Edmonton, you cannot go to the Federal Court or any other court to say I suffered damage to my reputation, my livelihood, and so on.

These are some of the areas in which on the overall approach we're good, and on the details we've fallen seriously behind.

The Chair: Thank you kindly.

The chair's going to use his discretion and jump in here.

Ms. Stoddart, does anyone from your staff have with them any of the latest material on your human resources shortfall and also the backlog on files with them here today?

Ms. Jennifer Stoddart: I believe we do, Mr. Chairman. We distributed some in the context of the appearance for the supplementary estimates, so we have that on human resources, which we could distribute to you.

● (1620)

The Chair: I wonder if someone could be prepared just to come to the table if they have to to be able to—

A voice: I could.

The Chair: You will? So we will be prepared to deal with that.

Ms. Jennifer Stoddart: And we have some material on the backlog.

The Chair: There was another item. In the joint audit that the Office of the Privacy Commissioner did with the Auditor General, where you presented the two excellent reports, both the Auditor General and yourself, with regard to four different departments, one of the concerns that you raised was pretty serious. It was that the legislation under the Canadian Elections Act provides that the birth date of electors now be shown on the electoral list. I think there were also some statements that some of this information was found in the hands of those who maybe shouldn't have it. When the matter was before Parliament, did the Office of the Privacy Commissioner identify that this was a potential problem, and did it appear before the committee or make any representations with regard to those amendments?

Ms. Jennifer Stoddart: Yes, to the best of my recollection, Mr. Chairman, I appeared twice. Once was with the director general of elections to talk generally about the use of identifiers and how they were handled in the context of defining who was an eligible voter. That was with the House of Commons committee. Then once the draft legislation was passed, I appeared at a Senate committee, as I remember, with the assistant commissioner from Ontario to express my concern about the full birth identifier, as the Ontario practice was the year only. This is from recollection. We could supplement that for you, but I did express concern about that.

The Chair: Okay, and that's the practice, to monitor evolving issues that may have some privacy considerations?

Ms. Jennifer Stoddart: Yes, absolutely. That's what our staff does.

The Chair: Mr. Wrzesnewskyj, please. Second round, five minutes.

Mr. Borys Wrzesnewskyj: Thank you, Chair.

Commissioner, why was the RCMP's Project Shock database closed down? What were the reasons given?

Ms. Jennifer Stoddart: Well, once we had announced our intention to audit and once my staff began to discuss this with the RCMP, they came to the conclusion with us that many years after 9/11—it was set up in the context of 9/11, in the months following 9/11—they didn't need that particular information in an exempt bank and could therefore close it down. So it was in the context of our audit.

Mr. Borys Wrzesnewskyj: So the explanation is that it was excess information, as opposed to information that was garnered in a way that wasn't allowed or required. Is that correct?

Ms. Jennifer Stoddart: I haven't reread our audit report since we launched it, but as I understand it, it was information that was no longer relevant to their needs; it was no longer useful. This was information that they thought might have been of strategic importance in 2001, but certainly isn't now. And it had never been reviewed, so that for most of it, I gather, the exempt status was removed.

Mr. Borys Wrzesnewskyj: Were gentlemen like Mr. Arar perhaps on that database?

Ms. Jennifer Stoddart: I don't know on what particular database Mr. Arar may have been.

Mr. Borys Wrzesnewskyj: Well, I'm asking about this Project Shock database that the RCMP closed down once you had begun looking at it. Was he on that particular database?

Ms. Jennifer Stoddart: I don't know. I simply don't know personal information about who was in the database.

Mr. Borys Wrzesnewskyj: Okay. Was that database shared with foreign governments?

Ms. Jennifer Stoddart: I'd have to look into the report. I don't remember that it was, but it doubtless could have been under Canadian law.

Mr. Borys Wrzesnewskyj: When you look into that report, could you also verify whether any of the other so-called closed databases had information that was shared with foreign governments? In this particular case, could you also look into finding out, if in fact it was shared, which governments that information was shared with and whether those governments have been informed that the particular database, because of the problematic nature of the data that had been gathered, has been closed down here, that it's not valid, and that foreign governments should no longer be using those databases?

● (1625)

Ms. Jennifer Stoddart: Yes, certainly, we will look into that and get back to you.

Mr. Borys Wrzesnewskyj: As a bit of a sidebar, we talked about genetic information and the sharing of information between countries, and obviously in North America a lot of that goes on.

I understand that as of a couple of weeks ago, Canadians travelling back to Canada who land in transit in the United States are actually being pulled into a separate line, and equipment has been set up and Canadians are being compelled to have their fingerprints and their irises scanned to be entered into a U.S. database.

Have concerns of that nature landed in your office yet?

Ms. Jennifer Stoddart: I don't recollect that we've had specific complaints or been notified that this is happening at this time. Again, we can check to see, but not that I'm aware of.

Mr. Borys Wrzesnewskyj: I was one of those stunned Canadians, by the way, who was pulled aside with all Canadians off a plane and required to do that.

The Communications Security Establishment within the Department of Defence is probably the most top-secret department within Canada. It has the capacity to electronically eavesdrop in ways no other government agency has. Have you ever done a full audit of that particular department?

Ms. Jennifer Stoddart: Yes, we did an audit in the last year, and I believe the results of that audit will be coming out in our next annual report.

Mr. Borys Wrzesnewskyj: Were there any significant concerns or areas of particular concern?

Ms. Jennifer Stoddart: Well, my annual report will be coming out soon.

Mr. Borys Wrzesnewskyj: We look forward to seeing that.

The Chair: I think we're there. I apologize.

We're going to have to move on to Mr. Hiebert, please.

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

It's a pleasure to see you again, Ms. Stoddart.

When you were before us in 2007 and 2008 we were asking you questions about your human resources situation, so hopefully it won't come as much of a surprise that we seek an update on the status of that situation.

We should always start with the big numbers. How many current investigations do you have ongoing?

Ms. Jennifer Stoddart: I believe it is 1,134.

Mr. Russ Hiebert: We are down slightly from where we were a year ago.

Ms. Jennifer Stoddart: Yes.

The Chair: I apologize, Mr. Hiebert. I won't take it off your time.

Just for clarification, are these just files assigned or actual investigations commenced?

Ms. Jennifer Stoddart: These are active files with my office.

The Chair: No, we have to split hairs here, because I believe there was a situation where, if a file was put on an investigator's desk but they had not started any work, it was counted as active.

Ms. Jennifer Stoddart: If you'll bear with me, I can take you through all that with the greatest transparency. I can do both, but in what order? Would you like me to answer the personnel question or—

The Chair: This is to help the committee understand where you are.

Ms. Jennifer Stoddart: Can I start with the good news?

As you recall, the committee took a very direct interest in the human resources state of my office last spring and we said at that time that we were severely understaffed due to a very severe problem of retirement, flow-through, people moving on, etc., in spite of having a fairly generous budget. The figures showed that it was hard to retain employees. At that time my staff and I testified that we had measures in place that would turn those figures around, so I am very happy to tell you that we are now slightly over our quota of employees as requested in the budget. We had about 120 in May and we now have 161, which was our goal.

I'm particularly pleased with the fact that in the various categories where the Government of Canada asks us to make special efforts, we're well over the targets to hire aboriginal people, people with disabilities, and visible minorities. The vast majority of those 124 positions are bilingual positions, so we have a very good cross-section of Canadian society. We did make some progress in the last eight months.

I thank you for your interest, and I think we are in much better shape for the future than we were in a situation of constant staff turnover.

● (1630)

Mr. Russ Hiebert: Speaking of which, what is the current turnover rate? In the past few years it was about 40% and your comment at that time was that it was equivalent to the public service. Can you give us some indication as to what the current turnover rate is?

Ms. Jennifer Stoddart: I don't have that figure with me today, but I did see that we're under that now. We have a very low turnover rate and in the last few months we've been well below the general civil service turnover rate.

Mr. Russ Hiebert: Going back to the number of active investigations, how many do you have? Can you break them down by Privacy Act versus PIPEDA?

Ms. Jennifer Stoddart: We currently have 547 PIPEDA investigations and 662 Privacy Act investigations as of the end of January, so we have a few more Privacy Act investigations than PIPEDA.

Mr. Russ Hiebert: In the past you've identified that a large number of your Privacy Act investigations relate to people who are incarcerated.

Ms. Jennifer Stoddart: Yes, they do.

Mr. Russ Hiebert: What percentage or what number of the 662 Privacy Act investigations would be related to that issue?

Ms. Jennifer Stoddart: If we look at our last annual report, we received some 759 complaints under the Privacy Act in all, and 248 complaints received were against Correctional Service of Canada. That does not mean that those who made them necessarily were themselves incarcerated at the time. At one point we had a whole flux of complaints by prison guards. But there's a high correlation. So that's over a quarter; that's a third. In the last annual report, a third of complaints were against Correctional Service of Canada.

Mr. Russ Hiebert: What's the date of that report?

Ms. Jennifer Stoddart: That is the report for 2007-08.

Mr. Russ Hiebert: That's the number we discussed last year. Do we know if that's still an ongoing problem?

Ms. Jennifer Stoddart: There is a constant phenomenon, as far back as you can see in the Privacy Act, that one of the huge users of the Privacy Act is the incarcerated population.

Mr. Russ Hiebert: I'd love to have that updated information.

The Chair: This is your last question.

Mr. Russ Hiebert: Is there any backlog with these investigations?

Ms. Jennifer Stoddart: Yes, there is unfortunately a backlog. We have decided to opt for the definition of less than one year, in terms of files being backlogged, because I think it was inaccurate and possibly misleading to say they're not assigned, and if they're assigned, that doesn't mean they're going to move, and so on. So we've taken a chronological criterion. In terms of the Privacy Act, of the 633 complaints as of last week, 270 are less than a year old, and the majority—363 complaints—are over a year old.

We do have in place a strategy by which, at the end of this fiscal year, there should be only 320 complaints, and by 2010 the backlog should be eliminated in both acts. So we're on target for reduction.

● (1635)

Mr. Russ Hiebert: So you're saying over half of them are backlogged, are over a year old.

Ms. Jennifer Stoddart: Yes. Right now, over half of them are over a year old.

Mr. Russ Hiebert: Do I have more time, Mr. Chair?

The Chair: Yes.

Mr. Russ Hiebert: That's a very large number.

Ms. Jennifer Stoddart: It is a very large number. Of the many challenges that my office has dealt with in the last few years, this is the last very serious challenge that is before us. It's a challenge of great magnitude. There's a similar backlog in PIPEDA.

Mr. Russ Hiebert: How do you explain the backlog? You have more staff than you've ever had. You had 120 staff last year, and now you have 160 and lower turnover. How do you explain?

Ms. Jennifer Stoddart: Unfortunately, the backlog is kind of like an iceberg growing. It grows very slowly, but it grows imperceptibly over years, and once you have it, it's hard to get rid of.

The backlog grew over the last few years when there were great administrative challenges at the Office of the Privacy Commissioner. For years, up until now, we have never had a full complement of investigators for various reasons. One was that we couldn't get financing for more investigators until we put our house in order, and that took several years, as you'll remember. A second was that we got the financing for new investigators, but then we were in this turnover mode largely due to the rarity of investigators as a specialized occupational group in the very specific Ottawa labour market. This was combined with the issue of retirement in a certain cohort of people.

However, this fall we have been able to hire 20 investigators as a group, and I think we have a complement of about 42 investigators. We have a whole influx of new people that are being trained in January and February and will start working mid-March. The backlog grew in the past, but I think now, with a full complement of human resources, we can go ahead in the future and attack it successfully.

The Chair: Colleagues, I allowed that to go on a little longer than I otherwise would have, but I think it is important that everyone hear about the challenges that are being faced here and why we've asked the Privacy Commissioner to keep us abreast of progress. When you have such a high turnover, you're getting a fair number of people whose productivity rates are low to start off with.

It's going to take some time, I'm sure, but we need to have the assurances that you have the resources available to you and that Treasury Board is also working collaboratively with you to make sure that you get the people you need when they're needed.

Ms. Jennifer Stoddart: Thank you.

The Chair: We'll move on to Madam Thi Lac.

[*Translation*]

Mrs. Ève-Mary Thaï Thi Lac (Saint-Hyacinthe—Bagot, BQ): Thank you, Commissioner. This is the first time I've met you, even though you've appeared before the committee on a number of occasions.

Earlier you said, in response to a question from my colleague Ms. Freeman, that your office has no obligation to protect the data gathered by the various departments. I imagine that standards are also their responsibility.

Ms. Jennifer Stoddart: Standards, with respect to privacy and security issues, are the domain of the Treasury Board, which makes the rules. Our role is as a commentator: we file complaints, we conduct audits. From time to time, we state that there are problems in the management of personal information, but it is up to the departments and agencies to protect and manage their personal information.

Mrs. Ève-Mary Thaï Thi Lac: Is there currently a standard procedure with regard to standards? If they come from the department, as you say, from the Treasury Board, is there a standardization of standards laid down in the various departments?

Ms. Jennifer Stoddart: Pardon me?

Mrs. Ève-Mary Thaï Thi Lac: Is there any uniformity, in the various departments, with regard to information gathering or protection?

Ms. Jennifer Stoddart: Practices vary somewhat among the departments and agencies. I can refer you—because it's more recent—to the special report that I made public last week together with the Auditor General. These are two concurring reports. Each commissioner's office has its own mandate, its specific mission, but one of the messages, which was the same in both cases, was the importance of Treasury Board's leadership as the central agency that defines and enacts standards with regard to privacy, training and resources to ensure that what happens to personal information is reported. We said that this leadership left something to be desired and that we expected the Treasury Board to take a firmer, more directive stance and to take a closer interest in what happens to the personal information gathered in the various departments under its responsibility.

● (1640)

Mrs. Ève-Mary Thaï Thi Lac: Have you considered common procedures for improving the protection of that information?

Ms. Jennifer Stoddart: We've worked together with Treasury Board in recent years. That's the specific role of the Assistant Privacy Commissioner. Under the act, we cannot stand in for the Treasury Board. I could draw your attention to the fact that, year after year, we say that training for Canadian public servants on privacy matters is inadequate. Staff appears to be overworked, overwhelmed by privacy issues. Authorities do not ensure that people are trained in this area. They don't ensure that a course on privacy is mandatory, as we request.

Mrs. Ève-Mary Thaï Thi Lac: I have one final question. Are there any decision-making powers that could be granted to you so that your office could increase protection for citizens' personal information?

Ms. Jennifer Stoddart: A number of critics of my office and of the Personal Information Protection and Electronic Documents Act have said before this committee that they thought the commissioner's office should be a tribunal, as in Quebec, Alberta and British Columbia. I've answered that the present model is fine with me for the moment. I haven't yet explored all I can do under this act. However, toward the end of my term, which is rapidly approaching, I intend to ask that we once again examine this issue of personal information protection in the private sector because Canada is currently the only major country that has a commissioner's office without power of order. However, we can appear in court. That's working very well for us for the moment. However, I think we should take another look at that issue.

The Chair: Mr. Poilievre.

Mr. Pierre Poilievre: Thank you for coming and thank you for the presentation made by your office a week ago. It was a great pleasure for me to talk to you and to hear what you've been doing.

I think Canadians are more interested in this issue, particularly with modern credit card payment methods and innovations by people who want to do bad things. It also has to be acknowledged that they are creative, even though we aren't entirely happy about that creativity.

[*English*]

My questions relate to the four organizations you focused on. You mentioned in 1.1 of your summary that the Office of the Privacy Commissioner examined the key elements of the policy frameworks of Elections Canada, Human Resources and Social Development Canada, Service Canada, and the Canada Revenue Agency. Collectively these institutions manage extensive personal information on just about everybody in Canada. Is that why you selected them for this audit?

● (1645)

Ms. Jennifer Stoddart: No. In fact they were selected by the Office of the Auditor General, who was undertaking an audit for reasons of her own. Her office approached my office and said that given that these particular agencies also have a lot of personal information on Canadians, we might like to do an audit at the same time, from our point of view. Then we could publish a report jointly or together about what we see from two different points of view. That's how it came about.

Mr. Pierre Poilievre: Okay.

What other agencies did you consider, or did the Auditor General consider, including in this particular audit?

Ms. Jennifer Stoddart: My understanding is that this was it. That was what the Auditor General approached us with. I don't know how her office functions in terms of the audit. Certainly, from my office, we audit various government agencies every year on an ongoing basis. Those are audits we do alone as part of our regular functions.

Mr. Pierre Poilievre: All right.

Now, I was reading through at point number 1.11 here, on page 7. You indicate that Treasury Board Secretariat monitors all institutions subject to the Privacy Act, through its public accountability instruments. TBS did not rate accountability for privacy as strong for any of the 46 institutions that it recently reviewed. So that's a pretty high failure rate for privacy.

Ms. Jennifer Stoddart: I thought it was interesting, because it showed that even TBS agreed with our analysis that accountability for privacy needed to be strengthened in the government.

Mr. Pierre Poilievre: And to credit TBS, at least they're willing to offer a frank assessment.

Ms. Jennifer Stoddart: Yes.

Mr. Pierre Poilievre: So there's lots of work to be done.

Ms. Jennifer Stoddart: Absolutely.

Mr. Pierre Poilievre: So where do we start?

Ms. Jennifer Stoddart: Treasury Board has our recommendations. We are waiting for the results of what is called a policy suite renewal, and we encourage Treasury Board to move on that. That's the continuous updating of privacy management guidelines for departments. Certainly if the government interested itself a lot more in the compulsory training on personal information protection, there would be fewer incidents or problems. There would be a heightened awareness by employees all through the government on this.

If it strengthened what are called its ATIP shops, which share the responsibility for access to personal information and access to other information, and where people—we met with them recently—feel under great pressure because of the interest in their personal information.... I can't speak to access—Mr. Marleau can do that. But certainly Canadians have a heightened awareness of personal information—where it's going, what's being done with it, and so on—and this creates new challenges for many of the workers in this area.

Mr. Pierre Poilievre: So you think training plays an important role in improving the system?

Ms. Jennifer Stoddart: Yes. I think training is an overlooked key to improving personal information protection. Because a lot of this comes out of the use of technology, I think we tend to use and look for new technology to solve the problem, and of course there's always someone who comes and tells us that if we just buy this technology, it will solve the problem.

But if we look at, for example, the self-reported breaches that come to my office from private sector organizations, some 40% of them have to do with just human error. This happens often in institutions where there's a big turnover of employees, and they don't have enough training, so they just forget. They're doing too many things at once.

To come back to your question, yes, if you trained civil servants better, I think you would reduce the risk to personal information.

The Chair: Thank you.

We'll have to move on now to Mr. Siksay, please.

Mr. Bill Siksay: Thank you, Chair.

When I was last questioning you, Ms. Stoddart, we were talking about the enhanced driver's licence program in B.C., and you listed a number of concerns that you had and that you'd raised about the enhanced driver's licence. Will any of those concerns have been addressed before the program goes into operation in March?

● (1650)

Ms. Jennifer Stoddart: There is, shall we say, an ongoing dialogue, Mr. Chairman. We learned last week that the trial database, which was going to be shared with the United States, or situated in the United States just for the trial of those 500 people who've signed up, was being repatriated into Canada, with the firm assurance that henceforth all personal information of Canadians will be permanently housed in Canada and it will be queried at the border point for the screens of the agents.

But I don't think we have—and I'll ask my colleague to complete this, since she's much closer to this project—enough information for the moment about how the trial is working. There are issues concerning the distance at which you can read this information, how well the sleeve is working, and whether the suggestion of another of my colleagues—to have an on-off switch, so you turn the emitting function on or off at the border—can be taken up in a useful time.

Perhaps my colleague can add something.

Ms. Chantal Bernier: I would simply add that indeed it is a work in progress. Last week the privacy commissioners of Canada were together in Ottawa and decided to create a working group precisely to systematically address these concerns together in a concerted fashion.

Mr. Bill Siksay: Do I understand correctly that the pilot project is only involving 500 volunteers?

Ms. Jennifer Stoddart: That's my understanding. It's going on in B.C; it involves 500 volunteers, and it is still being studied.

Mr. Bill Siksay: Is an RFID chip part of this enhanced driver's licence?

Ms. Jennifer Stoddart: Yes, it is.

Mr. Bill Siksay: Is there any other government-issued ID that contains an RFID chip that you know of?

Ms. Jennifer Stoddart: Doubtless there would be in many secure establishments, but I don't know offhand which ones; we haven't inventoried them. But it's getting to be a fairly commonly used technology.

Mr. Bill Siksay: Is that something you plan to do more work on, given the kinds of concerns you've raised about RFIDs? Is there a timetable on that?

Ms. Jennifer Stoddart: It's an ongoing concern of ours. It was one of the big themes of our annual report about two years ago.

Certainly as RFIDs spread through the marketplace we will be monitoring them very closely. Right now we understand they're being introduced into the merchandise supply chain at the pallet level. That is acceptable to us, if it stays at the pallet level. Let's say goods come from Asia. A certain percentage of them are lost at the dock, in transit, in shipping, with the trucking and so on. They are damaged and can't be used. There's a fair amount of wastage to wholesalers and retailers. We've been told that the RFID would help to individually track each pallet. I also believe there are national security reasons for tracking pallets of goods because you don't know exactly what they contain. That is fine.

The problem is when you break the goods out of the pallets. Let's say there are shoes being sent from Brazil. Do you have an RFID in each shoe so you can account for theft, people walking into the store putting on new shoes and walking out? If so, the privacy implications are enormous. There is one unique identifier in every RFID that can emit your location to a reader. If there's not some way of either preventing the RFIDs going in at an item level or turning the RFID off at the point of purchase securely, you could track where people are going or link it up to the card they paid with.

Mr. Bill Siksay: I have one more quick question.

One of the things you talk about in the report is the no-fly list. You said that you did a privacy impact assessment of the passenger protect program, but you also talk about doing an audit of the privacy management practices of the passenger protect program. I'm wondering what the difference is between those two things. It sounds like one's been done and one's coming up. What's the one coming up going to look at that the completed one didn't?

● (1655)

Ms. Jennifer Stoddart: The one coming up is going to look at how this system was administrated—for example, how many people went through it, the criteria on which they could fly or not fly, how many made use of the recourses in what I think is called the Office of Reconsideration. It's basically how the program is administered from a privacy point of view.

Mr. Chair, could I ask my colleague Lisa Campbell to talk to you about a case we're monitoring in the Federal Court on the do-not-fly list?

The Chair: Quickly, please.

Mrs. Lisa Campbell (Acting General Counsel, Legal Services, Policy and Parliamentary Affairs Branch, Office of the Privacy Commissioner of Canada): It's an interesting case. The name of the case is Hani Al Telbani against the Attorney General of Canada and Transport Canada. It's the first challenge in court, that we know of, to Canada's no-fly list. At the moment they're exchanging documents. An interesting side issue is that the applicant has asked for access to Transport Canada's documents. That's really what's at issue; he wants to know why he was denied boarding a plane. He asked that his name not be published, and the media and the Department of Justice intervened and said that because of the open courts principle his name should appear. He's in an interesting situation of perhaps never knowing why he couldn't get on a plane but his name is associated with this list.

The Chair: Okay, that's helpful.

Mr. Wrzesnewskyj, you have five minutes.

Mr. Borys Wrzesnewskyj: How many foreign governments do we share Canadians' personal files with?

Ms. Jennifer Stoddart: I can't answer that question, Mr. Chairman. I've pointed out many times that the Government of Canada has a very opaque system for sharing personal information with governments abroad. It's one of the recommendations for reform of the Privacy Act.

I think the law talks about an arrangement or an agreement—that's a fairly informal way of agreeing to share personal information, as compared to, for example, placing before Parliament, even just for its notification, all the MOUs with foreign powers as to what kind of information we share. It's really impossible to tell exactly in detail what information is shared.

Mr. Borys Wrzesnewskyj: So we're in a current situation where even you, as the commissioner in charge of privacy, can't tell us how many governments and with which governments in particular the Canadian government is sharing personal, private files of Canadians. Is that correct?

Ms. Jennifer Stoddart: Yes, that is correct.

Mr. Borys Wrzesnewskyj: Do we know what kind of data it shares with those countries? If we don't know the full list of countries, do we know what the limitations are on the type of data it would be sharing with this unknown number of countries?

Ms. Jennifer Stoddart: I don't believe the Privacy Act places any limits on the kind of information that can be shared abroad.

Mr. Borys Wrzesnewskyj: This appears to be probably one of the largest holes that need to be addressed.

Going back to a different part of your audit, dealing with passports, it was noted that there was a whole series of security issues and concerns, privacy breaches or breaches involving passports. Do you have a numerical breakdown of how many involve passports that were lost and stolen—which is one type of category—and how many actually involved internal breaches, whether within the offices here in Canada or in our missions abroad? Do we have a breakdown between the two?

Ms. Jennifer Stoddart: My report didn't include such a breakdown. Now, the passport office itself may have that kind of breakdown. We were looking at their practices, their approach to protecting privacy. Any particular incidents would be tracked by that agency.

Mr. Borys Wrzesnewskyj: I noted that the report also stated that in many of our missions we use locally hired staff, and in a number of those missions it's just impossible to do proper security background checks on that staff. Is there a list that can be provided of how many Canadian missions abroad are using locally hired staff that we have no background checks on?

● (1700)

Ms. Jennifer Stoddart: Doubtless one could be by DFAIT. We simply did a sampling of a couple and found this, but we don't have an exhaustive list.

Mr. Borys Wrzesnewskyj: Perhaps this is another area that should be looked at.

In those countries where we are able to establish security clearances, are they based on information provided by the host country, or are they independently verified by our own staff? Are we actually asking a foreign government to provide us with security clearances for people who might have access to sensitive information within embassies and consular sections?

Ms. Jennifer Stoddart: My understanding from the study we did, which focused on personal information protection, was that when we talk about security clearances we talk about them in terms of Canadian standards. This means meeting the independent standard the Canadian government sets rather than simply saying that in another country, if the other country says that they pass their security clearances, they pass Canada's. Again, I think DFAIT could give you the detail you're looking for.

Mr. Borys Wrzesnewskyj: There were some high-profile cases of countries that are allies of Canada where it appeared they had government agents using Canadian passports. Has it ever been determined how Canadian identification, passports of Canadians used by foreign agents, had been acquired? Have we ever delved into that?

Ms. Jennifer Stoddart: I don't think my office has ever looked into that, no.

The Chair: Thank you very much.

Mr. Dreeshen, please.

Mr. Earl Dreeshen (Red Deer, CPC): Thank you very much, Mr. Chairman.

Thank you, Madam Commissioner, for coming here this afternoon.

As we are coming near the end, some of my questions are going to be somewhat disjointed, as they have been asked in certain levels before. Actually one of the things I'd like to talk to you about is something that Madam Freeman had mentioned earlier, and that had to do with identity theft.

You've addressed the threat that is posed by identity theft. Could you tell the committee your current view on the subject and address some of the recommendations that you would like to see included?

Ms. Jennifer Stoddart: Yes, I think with regard to identity theft there's a consensus. What I'm saying is neither new nor original. Identity theft is really one of the huge, serious law-and-order issues facing Canadians. The cost of identity theft has now just skyrocketed. A lot of it is borne by the intermediaries that are the credit card companies and the banks, but I think we have to look at this, because all this adds to the cost of Canadians purchasing goods and services through the use of credit.

There are very few Canadians who have not been the victim of some kind of fraud. And we use the term "identity theft" loosely, from credit card fraud right up to having your house sold out from under you, which has happened to some people. This is, I think, a priority for governments to act on. I've raised this question for a couple of years, and I would hope that this Parliament could return to the necessary amendments to the Criminal Code to help the police crack down on those who collect personal information for wrongful purposes more easily. There was a bill that was introduced, and I think there's one that is being reintroduced. So that is something very concrete that could be done.

Certainly education is important, and we mentioned the brochure we're developing. You can give it to your constituents if you think it would be appropriate. It is about how to prevent identity theft, how to be wary about this. March is fraud prevention month, so we cooperate with fraud prevention, the RCMP, an organization called PhoneBusters, to do a couple of activities. We have things on our website to raise awareness about this phenomenon.

Mr. Earl Dreeshen: And I suppose that's when you would tie in to some of the things that are happening with regard to Facebook, as well as with some of the problems? Could you elaborate on some of the concerns that parents should have in that regard?

Ms. Jennifer Stoddart: Yes. If I go to the children's online privacy issue, this has been a concern of many privacy advocates, many forward thinkers, for five or six years now, as we watch the Internet companies moving into the huge market representing our children and especially the group called "tweens", who are about nine to twelve. Some of you may have tweens. They have their own websites that are very lucrative enterprises. They spend a lot of time on these websites. We had funded some research into the privacy implications for children and last June we launched an initiative with our provincial colleagues to really step up the information going to children and going to their parents about what to do and what not to do online.

So we've started our own youth privacy website, which is in conjunction with provincial commissioners, and we've also started a youth privacy blog. And then there's a section for parents on what to know when your kid first starts going online. I think I heard the other day that children are online now at two. As soon as they can recognize a letter, I guess they're online these days. So it has been a big priority for my office in the last year.

● (1705)

Mr. Earl Dreeshen: Thank you.

You also mentioned provinces and so on. When you were talking about the tribunals that take place in Alberta, Quebec, and B.C., just how does that tribunal work? Could you explain how that differs from the process that is followed at the federal level?

Ms. Jennifer Stoddart: Yes, in the three provinces the commissioner administers what is called an administrative tribunal. For those who aren't from a legal background, it's like an informal mini-court specialized in that particular issue. In some of these cases, for example in Quebec, you will have lawyers appearing, arguing the cases. In others, such as in Ontario, most of the cases have what is called a paper hearing. They're done on paper. There can be a combination of both. The parties are named, so it would be Joe Blow against ABC Corporation in terms of how it handled his personal information, and then the decision is made public on the Internet, with "J.B. v. ABC Corporation". That's how a tribunal works. The commissioner in the tribunal or an adjudicator to whom he or she delegates their authority can then make a binding order—do this with Mr. Joe Blow's information; stop collecting this; put in proper safeguards, things like that. That order can be appealed.

The Chair: Thank you kindly.

We're going to have to move to your colleague, Mr. Lauzon.

Ms. Jennifer Stoddart: Okay, I can come back.

Mr. Guy Lauzon (Stormont—Dundas—South Glengarry, CPC): Thank you very much.

It's a pleasure to have you here, Ms. Stoddart.

I must confess that I'm a guest here, just replacing someone, but I find the conversation extremely interesting and fascinating.

In a past life I was a public servant myself, and one of the things we dealt with was the speed of service. That was one of the determinants of the quality of our service. You mentioned that you have a 12-month target, and if an investigation is completed before 12 months, you've met the target. The number you have that aren't meeting that target is considerable. I read somewhere in your report that your average investigation lasts 14.5 months. In my past life, which was in processing unemployment insurance claims, we used to process 90% of them within 21 days.

I just can't imagine that you would build in a target that would go out that long. I'll tell you why I say that. When I was in a position similar to yours, and I was explaining to the upper echelon why I couldn't meet those targets on occasion, they would ask if it takes longer to process a claim at the beginning of the claim than it does 14 months out. I ask you that question. Why would you not process the claim?

Actually, I had a friend lodge a complaint, and I don't know if he ever got an answer, but he certainly said to me, "It's been four months, Guy. Can't you do something about it?" When I inquired about the four months.... I don't think anybody gets an answer in four months.

I wonder if you could make some comments about that.

● (1710)

Ms. Jennifer Stoddart: Yes, I certainly can.

First of all, the backlog is a very serious problem. It's our number one challenge now, and everyone throughout the Office of the Privacy Commissioner is turning their minds to overcoming this.

Mr. Guy Lauzon: Does it take two years?

Ms. Jennifer Stoddart: Yes, but as I indicated, the ways to make it disappear quickly are not there. If you look through the recommendations I made for both of our laws, I would like to have greater discretion as to which cases I have to take and which cases I don't have to take.

There are two phenomena. With respect to the Privacy Act, we have a certain number of people who come several times, who make a complaint every year because they want to know something in general. If we could simply direct them to our website to get the answer there, and so on, we could focus on something that would be of greater benefit to everybody.

This is a bit different from unemployment insurance claims. You either get your unemployment insurance extended or you don't. A lot of people simply want to know things. Some just want to complain about the government taking 31 days to process the complaint, even though they have the answer to the complaint. Those we have to touch with. That's for the public sector. I would like some streamlining of the law, because the administration of Canadian government is very different from what it was 25 years ago.

Mr. Guy Lauzon: Would you consider making the norm 90 days? I would like to make it 30 days, but to give you the benefit of the doubt, wouldn't it be better to put the norm at 90 days and work towards that? If I have twelve months to do something, I'll probably take twelve months. However, if I have three, I'll do it in three.

Ms. Jennifer Stoddart: Yes, and I'm not the only privacy commissioner in Canada to have this problem. Unfortunately, even if you put in the delay at a year, if you don't have anybody to look at this....

I've told you some of the challenges in the public sector. In the private sector, the challenges on some of the issues are so technologically complicated that they will need five or six people and a tremendous amount of technical assistance.

Look at the Facebook complaint, for example. There are apparently seven million Canadians on Facebook. One organization made a complaint about some of its fundamental operations, its pretty basic operations. You can imagine that we have quite a few people on the Facebook complaint, because it's relevant to so many people. Those are just some of the challenges.

Mr. Guy Lauzon: But, you see, that would be built in. If you were doing 90% within three months—

The Chair: Sorry, but we have to be fair to all members.

Mr. Guy Lauzon: Sorry, Mr. Chair.

The Chair: Mr. Poilievre, please.

Mr. Pierre Poilievre: I would be prepared to cede a little bit of my time if Mr. Lauzon just wanted to finish up that last point, Chairman.

Mr. Guy Lauzon: I was just about to say that's built into the system. As an example, if your target was to do 80% or 90% of your claims within 90 days, for those harder cases—and we had those cases that went on for three months or whatever—the truth of the matter, with all due respect, is that you're almost building in failure if you're asking for 12 months. That was my point.

Thank you, Mr. Poilievre.

The Chair: Thank you.

Mr. Pierre Poilievre: I think that was a very good point to add.

My question is somewhat related. It concerns the comparative professionalism and success of government agencies and the private sector. Some might say there can be no comparison because the private sector deals with different kinds of information and perhaps less sensitive information than government. I would tend to disagree with those who would make such a suggestion.

We have banks that take very personal financial information, such as marital status, etc., to determine whether we qualify for loans. We have credit card companies that do the very same thing. We have credit bureaus, to which many private organizations have access, that have very private financial information included within them. We have counselling services, psychiatrists, and psychologists who keep extremely private and personal information about the daily lives of people.

Sometimes all of this data is contained in mass systems. I'm just wondering how government is performing in comparison to its private sector counterparts in protecting data and private information in the modern era.

● (1715)

Ms. Jennifer Stoddart: Unfortunately, I think we don't have the same indicators to measure them, but I think the Canadian government is doing fairly well.

When I make my reports, I focus, of course, and a lot of senior civil servants then get back to me, saying, “We did all these things well, and why are you just focusing on the part that we didn't do well?” Well, that's kind of my role. But overall I think the Canadian government has a good record in personal information handling.

Certainly senior civil servants are very aware of this issue and very sensitive to this issue. I think we're struggling a bit now because we don't have modernized approaches and modernized laws. We need, as I said, a little more leadership from Treasury Board, but then we remember that government and places like the income tax department have been dealing with confidentiality for years and years.

There are some places in the private sector, but not banks.... You can say that banks have been dealing with confidentiality, but they probably haven't been dealing with the sophisticated security issues the public sector has. That may be a bit ahead of them because of the strategic and military experience of the Canadian government.

I think the Canadian government stands up quite well when you look across the world at how various governments use their information, and it stands up well in comparison with our own private sector. It also stands up well in its respect for privacy rights of citizens generally. I'm not saying there aren't things that can be improved, but this traditionally has been an important part of Canadian life.

Mr. Pierre Poilievre: My second question is also related to private versus public sectors and privacy protection. My question concerns your experience in examining the work of identity thieves. Do they succeed in stealing identities more often by use of government-issued documents like driver's licences and social insurance cards, or by use of documents issued by the private sector, like credit cards, bank cards, or receipts as record of payment, and birthdays? What is the source of the modern identity thieves' craft?

Ms. Jennifer Stoddart: Mr. Chairman, I'll ask our general counsel to answer that. I think she may have seen more data on that than I have. Thanks.

Mrs. Lisa Campbell: That's a very good question. This is how it works: Data brokers have become an industry unto themselves. Personal information is now worth money, and it usually passes through many hands. There's not one identity thief, but several: there's the person who collects it, the person who sells it, and the person who makes money off of it. Ultimately you need to get to a valid piece of usually government-issued ID. But to get there, often what's collected is invalid, stolen, or borrowed pieces of personal information that can come from a wide variety of sources. The private sector is often where it originates, but usually identity thieves will need some valid piece or what looks like a valid piece in order to do a legitimate transaction. We have recommended a wide range of approaches, from better personal information handling practices to more restrained collection to disposing of information when you no longer need it, and then, ultimately, to criminal sanctions for the very worst case of identity theft.

Does that answer your question?

Mr. Pierre Poilievre: You gave me a spectrum.

The Chair: Mr. Poilievre, we're already at six and a half minutes. But you've shared some, so that's okay. Those were good questions.

Mr. Pierre Poilievre: Is there not a way I could just get one final clarification there?

The Chair: You could get on the list again.

● (1720)

Mr. Pierre Poilievre: Okay, consider me on the list.

The Chair: Okay.

Mr. Siksay, please.

Mr. Bill Siksay: I've been thinking here, and I have just a couple of quick questions. Will the review you're now doing of the no-fly list program include the issue of racial and religious profiling as regards how that list has been administered, which has been a concern for some folks?

Ms. Jennifer Stoddart: I would think it would. I'm looking at my colleague because she supervises the department. I haven't seen the details of it, but I would think if that kind of profiling was going on, it would come out in our audit.

Mr. Bill Siksay: I have another quick question. You have called for a parliamentary review of the no-fly list, and that hasn't happened. Do you still think that's an important piece of work that needs to be done on the no-fly list?

Ms. Jennifer Stoddart: Yes, it is. Now that we have it before the courts, and given that there are so many issues—we just talked about identity theft and other things—it will be interesting to see what happens to this court case. Before you do a review, maybe wait for our audit, and then you will have more information.

Mr. Bill Siksay: I have a final quick question. You talked about the large number of complaints from people in the incarcerated population. Has that always been the case since the introduction of the act, or was there a turning point at which that began? Has there been any analysis of that trend line that would tell us that this is a new phenomenon, or is it a phenomenon that came from the very beginning of privacy?

Ms. Jennifer Stoddart: As far as I know, we haven't done one. We could go back to the annual reports. Certainly more of this has been reported in the last year. It's gone up in the last few years. But I've heard, anecdotally, for example, from people who were involved in writing the act—senior civil servants who were young civil servants at the time—who said that it had always been the case that the incarcerated population made use of the Privacy Act from its very beginning.

Mr. Bill Siksay: So we don't know if there's some failing in another program that is disappearing, through which some of those concerns might have been channelled or answered in a different way before they became privacy requests, or whether something changed along the way that made it more likely to happen now. There's just annecdotal evidence.

Ms. Jennifer Stoddart: Well, we haven't looked into it. Given the challenges and particularly the backlog of complaints, we try to focus on our own work, but it might be an interesting study for someone to see what has changed in the life of those who are incarcerated such that they increasingly turn to the Privacy Act. However, that is not a question we've asked.

Mr. Bill Siksay: Thank you.

Thank you, Chair.

The Chair: Thank you.

[*Translation*]

Ms. Freeman.

Mrs. Carole Freeman: Ms. Stoddart, are you aware that computer chips are now being inserted in credit cards—I don't know whether you've looked into this with regard to driver's licences—and that, if a consumer doesn't want to have a card with a chip because there's no way to know what information is retained by the chip and people refuse to disclose exactly what information is contained in the chip... Bank credit cards are under federal jurisdiction. In fact, the banks are under federal jurisdiction. Are you aware of that situation?

Ms. Jennifer Stoddart: No, I wasn't aware that people were able to ask what information was on the chip and that people had refused to tell them. If we have received complaints on that matter, I am not personally aware of it.

Mrs. Carole Freeman: Are you aware that the banks are about to put that—

Ms. Jennifer Stoddart: Yes. And that's something they've been planning to do for a long time. It should be noted that the Europeans have had that card for a number of years now. The Europeans appear to have fewer problems with bank card or credit card fraud. They expect that will enhance privacy.

Mrs. Carole Freeman: Are you aware of the information retained in those chips?

Ms. Jennifer Stoddart: No.

Mrs. Carole Freeman: You aren't aware.

Ms. Jennifer Stoddart: No. I imagine there are unique identifiers because it has to be activated with a PIN, which makes it possible to confirm that it's indeed the person to whom the card was issued who is using it, as is done in Europe.

Mrs. Carole Freeman: As regards the nature of the information, you're not aware of anything.

● (1725)

Ms. Jennifer Stoddart: No.

Mrs. Carole Freeman: In your appearance, you said that Canada didn't have legislation on e-crime or on e-mail or identity theft, although the Justice Committee has addressed that issue. Before the election, a study was done on the former Bill C-27.

You added that there was no legislation on the reporting of privacy risks. The worst of all—you win the prize—is that we have no idea of the number of countries with which we exchange personal information, nor are we at all aware of the scope of the personal information that is transmitted to other countries.

Ms. Jennifer Stoddart: I'm saying that, personally, I don't know, but I imagine the Department of Foreign Affairs and International Trade has an idea. There's also a publication entitled “Info Source”, which is a list of all government data bases. In my opinion, “Info Source” doesn't provide us with very useful information. It's simply a list of which we don't understand much.

I'm sure that someone in the federal government knows with whom we're exchanging personal information, country by country, but it's not me.

Mrs. Carole Freeman: Do you think the Privacy Commissioner may be one of the designated persons who should know, with regard to the transborder transmission of personal information, with which countries were doing business?

Ms. Jennifer Stoddart: Certainly, but I suggested in the report I prepared on the need to improve the Privacy Act that these kinds of agreements should be submitted to Parliament.

Mrs. Carole Freeman: But nothing is currently submitted to Parliament, if I understand correctly.

Ms. Jennifer Stoddart: No.

Mrs. Carole Freeman: Data transfers are made with other countries, and parliamentarians—

Ms. Jennifer Stoddart: They are made party to party between the officials responsible for the files.

Mrs. Carole Freeman: And Parliament isn't aware of that.

Ms. Jennifer Stoddart: No, Parliament isn't aware of it.

Mrs. Carole Freeman: This is personal information on citizens living in a country where they have rights.

Ms. Jennifer Stoddart: Exactly, the two countries can enter into a party-to-party agreement to exchange certain lists of personal information, which is perfectly legal under the present act, and there is no obligation to publish details.

Mrs. Carole Freeman: Nor is anyone required to publish and disclose.

I have another question, Ms. Stoddart, but it's nearly 5:30 p.m. So I believe I'm going to request adjournment.

[*English*]

The Chair: Ms. Simson, please.

Mrs. Michelle Simson (Scarborough Southwest, Lib.): Thank you, Mr. Chair, and thank you, Ms. Stoddart.

This has been a real education for me. I was newly elected in October, and I have done quite a bit of reading on this subject, but nothing quite prepared me for what I heard today.

I know you're just the messenger—and I appreciate the message—but I'm hearing that we're dealing with a 25-year-old act, we have civil servants who are undertrained, and it's your opinion that we're perhaps above average in some respect. That doesn't quite jibe with me, and I'm really concerned about your human resources position.

You said you're up to about 161 employees. Based on the current staffing levels, approximately how long will it take for that backlog to dissipate?

Ms. Jennifer Stoddart: We are calculating right now, if all things stay equal in our model, we should be able to eliminate that backlog by the first quarter of 2010.

Mrs. Michelle Simson: Based on the fact that we're dealing with extremely old legislation and technology is racing forward, do you know the approximate increase and the year-over-year increase in the number of complaints? Will the current staff levels be able to keep those in check?

And as a back-up question, how are the complaints prioritized—as you receive them, or are they reviewed and then some of the more egregious ones dealt with sooner? I'm not familiar with your process.

Ms. Jennifer Stoddart: Thank you for that question.

In fact we're redoing our process, because we're trying to push the limits of the present legislation a bit. We don't have a lot of discretion, but we do have some. Given the number of privacy challenges for Canadians, we want to make sure we get to the most significant ones first, while not neglecting any and maybe giving a shorter treatment time to the ones that may be less significant in terms of a general privacy policy.

As for the human resources, I'm very grateful for the human resources that we have now and I'm very happy that we've been able to hire some very able people. However, as you know, Ottawa is a hot market for talented people, and there is a challenge in retaining very bright people in a small agency where the opportunities for promotion are not those of a large department. That's just one of the challenges I have to deal with.

Another challenge in terms of human resources is that it's not just the numbers. I think the number I have is fine; it's training them. It's also being able to classify them within a very rigid system of classification that dates back several generations, because you're looking at people who have radically new skill sets to understand the new technologies and then translate them into what should be government action.

● (1730)

Mrs. Michelle Simson: Thank you.

The Chair: Mr. Hiebert.

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

I had an outstanding question dealing with the report from last year.

Ms. Stoddart, do you remember talking to us about a triage factor analysis grid that you felt would re-engineer the process of addressing these complaints?

Ms. Jennifer Stoddart: Yes, I do.

Mr. Russ Hiebert: You said that you were hoping to complete it by the end of the year. That was in 2008. Did you ever have a chance to complete that grid?

Ms. Jennifer Stoddart: Yes, we've completed that, and it's been piloted, as I understand, starting maybe a week or two ago. It's on its pilot runs.

Mr. Russ Hiebert: Is this part of your plan to reduce the backlog in the next year?

Ms. Jennifer Stoddart: This is part of our plan to maybe do a smarter handling of complaints, trying to give them the treatment they deserve in terms of their significance, their weight, of what they can add to our knowledge of privacy, trying to mediate complaints up front so that they don't go on and turn into a backlog, and do things, if we can, within 90 days.

We're doing some other things with the private sector. For example, if people have a complaint against a bank—and I'll use the bank because we all have several bank accounts and there are a lot of complaints against banks—we would ask if they have contacted the bank's chief privacy officer to see if they could settle this. Often the people have, so with the banks and other major respondents, like Air Canada and so on, we direct the people back to those organizations. That's now also increasing the rate of settlement.

Those are some examples of how we're putting this grid to work.

Mr. Russ Hiebert: In your presentation you talked about needing a complete overhaul of the Privacy Act. As you might know, for some time I've been one of the advocates for reviewing this legislation. We started on this last year and have made some progress.

When you talk about a complete overhaul, you're obviously talking about going beyond the ten fixes that you had proposed. What were you contemplating, beyond those ten fixes, when you were speaking about this?

Ms. Jennifer Stoddart: The other fixes? I'll just try to find them for you, because we have quite a few other ones. I'll just go down it, because this is a distillation of what is in a long paper that we published in 2006, and it's also a distillation of what some of the many expert witnesses say to you.

It says to look at clarifying in the Privacy Act government obligations regarding outsourcing and public-private partnerships, the delivery of service and programs, something that the Privacy Act doesn't speak to, outsourcing generally. And look at security arrangements. The Privacy Act per se does not obligate departments and agencies to make appropriate security arrangements. We say this is part of confidentiality and privacy. In PIPEDA we do talk about specific security arrangements. That would be another thing.

There are the questions some of the honourable members have been raising about the national security oversight framework. So what is the transparency, the accountability oversight over some of the national security agencies—the RCMP, CSIS, CSE, and so on. These were some of the recommendations we made to the O'Connor inquiry about oversight in the use of personal information in the RCMP, which have not been taken up for the moment.

I'm just going down the list to give you a flavour.

We believe that there may be other agencies and government bodies that should be subject to the Privacy Act. I was very happy that the Federal Accountability Act covered more agencies, but we think that there may be a few more that we could find if their activities were reviewed.

Access to people's personal information has come up in our dealings with the European Union. Actually, you have to be a Canadian citizen or present in Canada to avail yourself of your rights under the Privacy Act. This is a bit embarrassing when we're dealing with transborder data flow, API/PNR, agreements with the European Union. Now, we have—and I have been consulted on this—agreed that if European people, for example, flying into Canada had a complaint about the use of their API/PNR, CBSA would investigate, and then I would treat it as a complaint, although strictly speaking it doesn't fall within the Privacy Act.

● (1735)

Mr. Russ Hiebert: All right. There's a lot there.

How urgent do you think it is that we address these? We have the option of looking at the ten fixes, over which there is some dispute in regard to which of those ten we could implement. For the benefit of the members who are new to this committee, can you give us a sense of to what degree this urgently needs to be dealt with?

Ms. Jennifer Stoddart: Mr. Chairman, I picked the ten quick fixes on the advice of my staff because I thought they were important but also fairly easy and less multilateral; there were fewer multilateral implications of addressing them.

I know that the amendments to the Privacy Act are a long and contentious road to set out on, so if I could refer you to those ten recommendations, I think they still stand. They would be a net improvement, but they would be easier to implement than some of these others. You can imagine it for extending access rights and so on.

The Chair: Thank you.

Mr. Dreeshen, please.

Mr. Earl Dreeshen: Thank you very much.

Mrs. Kelly Block: On a point of order, Mr. Chair, I understood the meeting was to end at 5:30. I know I had this point of order at our last meeting, but I have arranged my schedule for other meetings on the understanding that this meeting ends at 5:30. Is it at your will that we continue meeting, or...?

I would like to move that we end this meeting.

The Chair: Okay. First of all, it's not a point of order, but the question is relevant so let me address it. Should there be a meeting of another committee, or even of this committee, a steering committee that was scheduled at a particular time right after our normally scheduled meeting, we would adjourn. However, meetings don't adjourn. We just have our time slot. We reserve this room as long as it's available. The meeting goes on. The members themselves decide that they want to go on. We still have Mr. Dreeshen, Mr. Poilievre, and Madame Freeman on the list who would like to speak with the Privacy Commissioner.

I think the answer to your question is that if it's getting repetitive, or if it's not relevant to the order of business before us, the chair also will shut down debate at that point. Having said that, I note that the committee is always the master of its own work. Should the majority of the committee wish to adjourn the meeting, then it would be up to a member to simply move that we adjourn. That would be the proper procedure. It's not debatable. We put a vote immediately and there we are.

Mrs. Kelly Block: I so move.

The Chair: Okay. Before I consider that motion, I would like to thank the Privacy Commissioner and her colleagues.

Mr. Pierre Poilievre: On a point of order, Mr. Chair, I think it would be more appropriate to thank them after we're done. If the meeting does go on, then they will be here longer—

The Chair: Thank you.

Mr. Pierre Poilievre: —and I think, of course, that to thank them now would be inappropriate. I would like them to be properly thanked.

● (1740)

The Chair: Yes. As for “properly”, once we adjourn there is no record of this.

Mr. Pierre Poilievre: Okay.

The Chair: Let's have a record that we thank them and that there are some undertakings.

Ms. Jennifer Stoddart: Yes.

The Chair: If you have any concerns about what those undertakings are, the clerk also has kept a record, and we would be happy to collaborate with you to make sure we get that. The information will be properly circulated to all honourable members.

I'd also like to indicate for all honourable members before you leave that the Privacy Commissioner has also brought copies of various reports, which are on the table off to the side corner. If you have the time, please take copies. There are the last two annual reports, I believe, as well as the Auditor General's report.

Thank you very much.

We have a motion to adjourn. It's not debatable and I'll put the question now.

Some hon. members: Agreed.

The Chair: 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
