House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 038 • 2nd SESSION • 40th PARLIAMENT

EVIDENCE

Thursday, November 19, 2009

Chair

Mr. Paul Szabo

Standing Committee on Access to Information, Privacy and Ethics

Thursday, November 19, 2009

● (0910)

[*English*]

The Chair (Mr. Paul Szabo (Mississauga South, Lib.)): This is meeting number 38 of the Standing Committee on Access to Information, Privacy and Ethics. Our orders of the day are pursuant to Standing Order 32(5), the annual report of the Privacy Commissioner for the fiscal year ended March 31, 2009, which was referred to our committee on Tuesday, November 17, 2009.

Colleagues, before I start, I'd like to introduce to you Dara Lithwick, an analyst who will be joining our committee for a while when our colleague Élise takes maternity leave, which will be starting at the appropriate time.

Welcome to you, Dara, and I hope you have an opportunity to help us.

This morning's witnesses, from the Office of the Privacy Commissioner, are Ms. Jennifer Stoddart, the Privacy Commissioner, and Chantal Bernier, the Assistant Privacy Commissioner. They are here to deal with two matters. One is the annual report and related matters. We will be excusing the commissioner after we deal with that part.

The committee also has an agenda item to address the government's response to our report on the quick fixes to the Privacy Act. We will have some discussion about that similar to what we had with regard to our report on the Access to Information Act.

That's just to give the members a heads-up on how we'll proceed.

Good morning, Commissioner and Assistant Commissioner.

Ms. Jennifer Stoddart (Privacy Commissioner, Office of the Privacy Commissioner of Canada): Good morning, Mr. Chairman.

The Chair: It's good to see you again. I must admit that it would be hard not to realize that privacy issues have been enjoying substantive attention in the public domain, which I think is extremely helpful because it will encourage engagement with the public as well as with legislators.

That's just kudos and a thank you for continuing to advocate on behalf of important privacy issues.

I understand you have an opening statement for us, and then I'm sure the members will have many questions for you. Please proceed.

Ms. Jennifer Stoddart: Thank you very much, Mr. Chairman.

Could I begin by simply informing the committee that the group of people accompanying me are on one hand some staff members who in the years they have worked at the Office of the Privacy Commissioner have never attended a hearing of the Privacy Commissioner. We realized, perhaps belatedly, that it was very important for them to see what happened and what the interaction was.

[*Translation*]

Moreover, as I was explaining to the chairman, we have Mr. Allassani Ouédraogo from the National Commission for the Protection of Data of Burkina Faso, which is now the first commission accredited according to African international standards. Mr. Ouédraogo is here with us in Ottawa to see what we do here and possibly to learn from us since both of our countries are members of the Francophonie.

[*English*]

Thank you very much.

The Chair: Welcome to our guests from Burkina Faso.

Ms. Jennifer Stoddart: Thank you.

On Tuesday, Assistant Commissioner Bernier and I had the privilege of presenting to Parliament our latest annual report on the Privacy Act. I believe it is an important document for all Canadians because it highlights some vital developments and future trends in public sector privacy. Through the lens of the audit and review and the complaints investigation work of my office during the 2008-09 fiscal year, the report explores the privacy challenges posed by two broad societal influences: national security initiatives and technology.

I will touch on key highlights of the report in a moment, and then I propose to share a few thoughts on the unresolved matter of Privacy Act reforms. First, though, I would like to underscore the principal message that emerged from our annual report.

That message is that privacy rights should not be at odds either with public security or with the use of information technology. On the contrary, we contend that measures to respect privacy must be integral to all these new developments.

First of all, I'd like to talk briefly about the FINTRAC audit. In this annual report, my office reports on what we discovered in privacy audits of two major national security initiatives: the passenger protect program, better known to Canadians as the no-fly list; and FINTRAC, the Financial Transactions and Reports Analysis Centre of Canada. Our FINTRAC audit found that the agency generally has a robust and comprehensive approach to securing the personal information of Canadians. However, our examination of the sample of files in FINTRAC's database turned up personal information that the centre did not need, use, or have the legislative authority to collect. In some cases, in fact, reports existed absent even a shred of evidence of money laundering or terrorist financing. Clearly, excess personal information should not be making its way into the FINTRAC database.

One of our key recommendations was that FINTRAC do more work with reporting organizations to ensure that it does not acquire personal data beyond its mandate. After all, it is a bedrock privacy principle that you collect only the personal information you need for a specific purpose.

Aside from the recommendation on data collection, we also called on FINTRAC to delete permanently from its holdings all information that it did not have the statutory authority to receive. We recommended that FINTRAC analyze all Proceeds of Crime (Money Laundering) and Terrorist Financing Act guidance issued by its federal and provincial regulatory partners to ensure that such guidance does not promote client identification, record keeping, or reporting obligations that extend beyond the requirements of the act.

We were very pleased that FINTRAC accepted 10 of our 11 recommendations. We had recommended that it strengthen its information sharing agreements with foreign financial intelligence partners by including mandatory breach notification and audit provisions, but the centre maintained that its efforts in this area were sufficient.

● (0915)

[*Translation*]

I am now going to discuss our Passenger Protect Program audit. A second audit summarized in the annual report relates to our examination of the Passenger Protect program. In general, we found that Transport Canada collects, uses and discloses personal information related to the program in a way that safeguards privacy. We did, however, identify a few gaps.

One related to the information that officials supply to the deputy minister, who is ultimately responsible for adding to or removing people's names from the no-fly list or Specified Persons List.

In light of the serious consequences flowing from every one of these decisions, we found that officials have not always provided the deputy minister with all the relevant information on which to base a sound decision.

Our audit also revealed that Transport Canada had not verified that airlines were complying with federal regulations related to the handling of the Specified Persons List. The risk of a breach was especially high for the handful of air carriers that relied on paper copies of the list. Further, we found that air carriers were not obliged to report to Transport Canada security breaches involving personal information related to the no-fly list.

The audit also found that the computer application used to provide air carriers with information on the no-fly list was not subjected to a formal certification and accreditation process designed to ensure the security of sensitive personal information.

We were, however, pleased that Transport Canada responded positively to all our recommendations.

[*English*]

We'd like to now turn to investigations and inquiries.

The annual report we presented to you this week also includes details of our engagement with Canadians through our public inquiries and complaints work.

Over the 2008-09 fiscal year, my office received more than 12,000 calls and letters from Canadians concerned about privacy issues.

With respect to concerns focused on the public sector, we received 748 complaints in 2008-09, down slightly from the previous year. The most common complaints related to problems people encountered in accessing their personal information in the hands of the federal government and to the length of time it was taking departments and agencies to respond to access requests.

In analyzing our caseload, we noted that technological glitches can have an extraordinary impact on the privacy of Canadians. For instance, we found that a hacker, using amateurish off-the-shelf software, was able to penetrate a computer at Agriculture and Agri-Food Canada, exposing about 60,000 personal data records of farmers using a federal loan guarantee program. But we were equally disturbed to discover, 26 years after the passage of the Privacy Act, that too many data breaches could still be traced to decidedly low-tech origins, from a briefcase left on an airplane to the careless mishandling of sensitive documents.

That said, I want to underline that the vast majority of public servants we have worked with across the government do take privacy issues very seriously.

[*Translation*]

I will now talk about the challenge the backlog presents. In all, our office was able to close 990 complaints files related to the Privacy Act during the fiscal year, up almost 13% from the previous year.

You will notice that we closed more files than we opened. That is due to a concerted effort to tackle a significant backlog of cases, which had driven up our treatment times from an average of about 14 months in 2007-2008 to 19.5 months in 2008-2009.

Our backlog challenge was exacerbated over the past fiscal year when we decided to redefine when a file is deemed to be in backlog, to more accurately reflect how long Canadians actually have to wait for service.

As a result of the redefinition, 575 files were backlogged in April 2008. Fortunately, through a significant re-engineering of our systems and processes, we managed by the end of the fiscal year to cut that number down by 42% to 333 cases. We are on track to eliminate it altogether by next March.

I will now discuss the Privacy Act reform. Over the past year, my office and this committee have also continued to work toward the modernization of the Privacy Act, to ensure it properly protects the fundamental right to privacy in the digital age. Reform of this statute is essential to meet the modern privacy needs of Canadians. And yet, despite our efforts and those of this committee, I confess to a measure of disappointment when it comes to the government's response to this committee's report of last June.

As we all know, Mr. Chair, updating antiquated privacy legislation and ensuring that privacy principles apply uniformly to the public and private sectors is becoming increasingly urgent in this globally interconnected era. Indeed, other industrialized democracies have already recognized this imperative. Australia, for instance, is rewriting its federal privacy laws so as to create a single set of principles covering government agencies and businesses alike, address emerging technologies, and introduce consistent new provisions on cross-border data flows.

The European Commission has announced that it will be re-examining its 1995 directive to see whether it is still capable of fostering the level of data protection required for the modern technological era. In light of the fact that our own Privacy Act is 12 years older, we can no longer ignore the need to make significant updates to our own law in order not to be left behind.

● (0920)

[*English*]

In summary, Mr. Chairman, I would like to end with a few words about the work of my office as we continue to move through 2009 and 2010.

I can tell you that we're already deeply engaged in several key files, all of them with significant impacts on the privacy of Canadians. Notably, with the 2010 Winter Olympic and Paralympic Games just around the corner, the challenge of integrating privacy and security will come to a head in an unprecedented way. We have already engaged security officials in a constructive dialogue to build privacy considerations into their security measures.

At the same time, we are taking a close look at Citizenship and Immigration Canada's plans to roll out initiatives using biometric information. For example, CIC is collecting fingerprint data from refugee claimants and is sharing it with other countries.

And we will continue to make known our views about Bill C-46 and Bill C-47, legislation to oblige wireless, Internet, and other telecommunications companies to make subscriber data available to authorities, even without a warrant.

Since the terrorist attacks of 9/11, Canada has seen a proliferation of new national security programs, many involving the collection, analysis, and storage of personal information. We fully appreciate that the underlying aim of many security programs is to protect Canadians. But as we will continue to remind Parliament and Canadians at every opportunity that it is critical that privacy protections be integrated into all such initiatives at the outset.

Thank you very much, Mr. Chairman and members of the committee. My colleague and I welcome your questions.

The Chair: Thank you kindly.

We'll move right to questions from the members.

We'll start with Madam Simson, please.

Mrs. Michelle Simson (Scarborough Southwest, Lib.): Thank you, Chair.

Many thanks, Ms. Stoddart and Ms. Bernier, for appearing before the committee and for all your fine work—I've been following it closely—and specifically for your report. It was very informative.

Getting right to the report, you referred to the Treasury Board Secretariat as having developed new privacy policies and guidelines. You specifically referenced a newly introduced policy on guarding personal information and new guidelines for information sharing agreements covering the exchange of information between government departments and with other countries and jurisdictions.

How much involvement did your office have in developing these new policies and guidelines? To what degree was your input sought?

● (0925)

Ms. Jennifer Stoddart: My recollection is that we were consulted several times on this. This dates back a certain time, but we certainly were consulted on it. In fact, we are regularly consulted on the development of Treasury Board guidelines that have to do with personal information protection. We have an ongoing relationship with that unit, which is usually under the supervision of my colleague Chantal Bernier.

Mrs. Michelle Simson: Thank you.

Are you personally or is your office satisfied that introducing or changing policies and guidelines...? In other words, do you believe that just changing policies and guidelines, as opposed to changing a statute that's over a quarter of a century old, affords Canadians adequate privacy safeguards?

Ms. Jennifer Stoddart: No, we don't. We're happy that there are policies, but policies are not law and policies are often of uneven application. It's clear, if it is a policy, that as a policy it's not quite as compulsory. A lot of our efforts—to which this committee has been a partner—are taking some of these existing policies and saying that if this is government policy, why couldn't it be in an updated Privacy Act?

I take the example of what's happening in Australia. One of the policies you mentioned about criteria for sending across borders personal information of Canadians held by the government and its agencies is one of the things that are going to be integrated into the new Australian privacy law.

Mrs. Michelle Simson: That's about what I suspected.

Did you want to go ahead?

Mr. Borys Wrzesnewskyj (Etobicoke Centre, Lib.): Yes, thanks, if you're done.

I have a couple of questions. In your report, I note that under "Institutions by Complaints Received", National Defence had 25. Do you have a breakdown on the various departments within National Defence where complaints were received?

Ms. Jennifer Stoddart: We could provide that to you.

Mr. Borys Wrzesnewskyj: That would be helpful.

Were there any complaints received against the Communications Security Establishment? That's probably the most secretive department we have in Canada. Nobody seems to know what they really eavesdrop on, so I guess it's hard to make a complaint if you really don't know what they're up to.

Were there any complaints against the CSE?

Ms. Jennifer Stoddart: My colleague is just checking the list to see if we see any.

I'd be surprised if there were or, if there were, if there was more than one, because, as you say, people don't know when their information is there. And people in national security have pointed out to me that if you suspect you're in there, the last thing you want to do is draw public attention to yourself by making a complaint.

So we don't see any this year.

Mr. Borys Wrzesnewskyj: And here's one of the problems. I'd be surprised, actually, if there were a complaint, because no one seems to know what they are actually up to, except that they've got probably some of the best technology in the world when it comes to eavesdropping electronically on Canadians.

When is the last time your offices did an audit of their databases and activities?

Ms. Jennifer Stoddart: It would be hard for me to answer that accurately right now, so again I'll get back to you on that, because I may be confusing CSIS and CSE. We did some preliminary checking—perhaps it was with CSIS, as I remember—and the preliminary analysis suggested that everything was correct in terms of personal information handling issues. But let me get back to you to be completely accurate.

Mr. Borys Wrzesnewskyj: Because this is a department within National Defence, I'm sure they share information with CSIS, but I'm curious about their actual protocols when it comes to privacy. How does this eavesdropping agency share its information with other countries that are engaged in eavesdropping? It's such a murky world. We don't seem to have any idea of what they're actually up to? Do we know what their protocols are, in fact?

● (0930)

Ms. Jennifer Stoddart: I certainly don't, and I don't know that my mandate would give me the authority to ask exactly what their protocols are.

My colleague has worked in national security for a while.

Can you respond?

Ms. Chantal Bernier (Assistant Privacy Commissioner, Office of the Privacy Commissioner of Canada): What I was going to add is that in fact this goes to one of our recommendations that there be a reform of the Privacy Act to put clearer definition as to how personal information can be shared with foreign governments. We agree with you that this area would deserve some attention.

Mr. Borys Wrzesnewskyj: This is something we probably need to spend a little time on. An agency that's extremely well funded has access to using some of the top technology, and we know where technology has gone in this area. With the computer capabilities, with the capabilities of eavesdropping, etc., we know where it's gone. Yet even our commissioner...no one seems to really know what they're doing, what kind of information they are after, how they're using that particular information, and who they're sharing it with. That's of great concern.

Ms. Jennifer Stoddart: Yes. There is an oversight authority over CSE who used to be a retired judge of the Supreme Court. I'm just trying to think...Monsieur Gonthier, but he just died recently. So there is some oversight built into it. And we met with Mr. Justice Gonthier about two years ago. He just wanted to be sure that he was applying the Privacy Act the same way as we were. So I found that was very positive. But he of course didn't tell us about his work because it's highly confidential and top secret.

So there is an authority, though, who does oversee some of the work of CSIS.

The Chair: Thank you.

Madame Faille, vous avez la parole.

[*Translation*]

Ms. Meili Faille (Vaudreuil-Soulanges, BQ): Thank you, Mr. Chairman.

Thank you, Madam Commissioner, for being with us today. Your report indicates that you are worried about the quantity of information, of data that are being kept without citizens' consent. Perhaps you know that your jurisdiction is currently being questioned with regard to frequent flyer client loyalty programs, plans such as Aeroplan.

On page 39 of your report, you mention that there are an increasing number of requirements on the part of the U.S. Department of Homeland Security which coordinates the USA Patriot Act. Under this legislation, businesses such as Aeroplan, whose head office is housed in Montreal, are required to transfer information from their database on people who have Aeroplan cards, when they communicate using USA telecommunications systems. Are you aware of this problem? How do you intend to approach this?

I think that the authorities involved are going to have to be redefined, that is to say who is allowed to transfer what and how citizens are informed. I am sure that a lot of people who have Aeroplan cards today don't know that when they travel in the United States, their personal data are transferred to that country. Has this problem been brought to your attention?

Ms. Jennifer Stoddart: No, not the problems involving Aeroplan specifically. However, we did discuss these matters a few years ago in one of our conclusions where we said that a credit card company affiliated with a major bank—

Ms. Meili Faille: I think it was the CIBC.

Ms. Jennifer Stoddart: Exactly.

It was transferring data concerning Canadians to the United States for processing. We concluded that since this had been explained when the credit card was obtained, this fell within the parameters of Canadian law and that the company or the bank in question had taken all the measures necessary to prevent illegal access. We know that data in the United States are subject to American laws. So that is how the matter was viewed in the past.

However, I'm not aware of the exact details concerning Aeroplan since this was not brought to our attention either through a complaint or in any other way, to my knowledge.

Be that as it may, I'd like to get back to another part of your question. You asked me if our jurisdiction was being called into question, if I am not mistaken.

I don't think that with regard to this, there are jurisdictional issues. There are in the case of insurance: certain American companies are challenging this. Moreover, when businesses such as Air Canada are concerned, whose head offices are located in Montreal, we collaborate fully with our colleague from the Quebec committee. For instance, one may say to the other that he or she could do this, or that this will be done, or suggest that we undertake action together. Recently, we went to Brussels concerning a matter involving doping standards. The head office of the body responsible for administering the antidoping program is in Montreal.

● (0935)

Ms. Meili Faille: Are you the body responsible for overseeing and certifying this type of action at this time?

Ms. Jennifer Stoddart: This matter does fall under our jurisdiction since this is an international matter. However, that does not exclude the fact that Quebec could also have jurisdiction over this matter. We want to work in a collegial way with our colleagues. And in the pursuit of friendly relations, we work in a complementary fashion. That is what we do with several provinces.

Ms. Meili Faille: I'd like to focus my question on the information being kept without the consent of citizens. The Canada Border Services Agency has a system known as the Advanced Passenger Information System. When they approach organizations such as the Department of Citizenship and Immigration, the Canada Border Services Agency and the RCMP, it seems that citizens are meeting with automatic resistance when they ask for information. It is only when they threaten legal action or complain that information is suddenly provided to them.

Have you noted an increase in negative first responses due to this resistance of organizations when the time comes to provide information to Canadian citizens?

Ms. Jennifer Stoddart: I am going to ask my colleague to reply because she supervises the administration of complaints in this area. She may have information on this topic.

Ms. Chantal Bernier: Indeed there is tension inherent to access and the protection of information, so that in our relations with certain federal agencies in particular, we note greater resistance because they are more concerned with keeping things confidential.

That being said, that is why the Privacy Act exists and why it gives citizens the right to request access. We are there precisely to intervene to facilitate access and decide whether the denial of access is well founded or not.

Ms. Meili Faille: That's fine. I simply want to ask another question.

I want to talk about a similar situation, which is when information is being kept without the consent of citizens. At Citizenship and Immigration Canada, when a permanent resident loses his or her card and requests a replacement or reports that the card has been lost, his name is automatically recorded in a system known as the secondary referral process. This person then finds himself in a system which means that whenever he leaves Canada and returns here, he is automatically searched and an investigation is done.

Have you had a chance to study this system? Do you deplore the fact that there is no way of getting out of this system? This is a system people are placed in automatically. I find this unjust and unjustifiable.

Ms. Chantal Bernier: We have not yet studied this system, but I take good note of your comments. This is the type of problem that falls within the purview of our mandate.

Ms. Meili Faille: Thank you.

[*English*]

The Chair: Mr. Siksay, please.

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

Chair, I wanted to begin by saying that I know there have been some challenges to you personally lately regarding your chairing of this committee, and I want to express my confidence in your work. I believe you serve this committee extremely well and very fairly. I just wanted to begin with that comment this morning.

I want to thank Ms. Stoddart and Ms. Bernier for being here yet again, and also thank you for the work in your annual report. There's a lot going on at the Office of the Privacy Commissioner and some very important work.

I wanted to go through the Minister of Justice's response to the committee on our report and get your observations about some of the points he makes.

The first one is in the fourth paragraph of the Minister of Justice's response to our report, where he responds to the idea of bringing the Privacy Act and PIPEDA in line. He seems to point out that there are two difficulties with that. One has something to do with the legislative mandate, that there's a problem deriving from the authority to carry out mandates from federal statutes, and the other is that there is some requirement around charter compliance.

I wonder if you could comment on those two points the minister makes.

● (0940)

Ms. Jennifer Stoddart: Yes. Thank you for that question.

Indeed, in reading that, I was very surprised at that reasoning, because while in a sense it is true, yes, that the commercial entities are not covered by the charter, more and more we are looking to try to converge the standards for personal information handling between the public sector and the private sector.

Indeed, I gave you two examples. Australia, which has often served as a model for Canadian law-making because of the similarities in terms of population, history, and constitution between the two countries, is in fact moving to such a converged system. On the other hand, the European Union, as I understand, with the implications of something called the Treaty of Lisbon, is going to move to a system where both of what they call the first and third pillars—that is their government, the European Union, as well as all the commercial activities, which were the basis of the European Union in the beginning—will be covered by the same data protection directives and policies.

So here are two very interesting political entities whose movement, in fact, presents another vision than that put forward by the minister.

Mr. Bill Siksay: In the sixth paragraph.... I think we've already talked this morning a little bit about this. It's the question about whether you need legislated requirements or if policy is enough. The minister uses the word “obliged”. Do you think “obliged” is a strong enough response to the requirements you saw for changes in the Privacy Act and legislated requirements in certain areas?

Ms. Jennifer Stoddart: Well, “obliged” means departments should do it, but one of the things we've been concerned about is that there's no clear sanction if they don't do it. There are a number of policies. Senior officials will say there are so many policies in the government that it's hard to comply with them all, but we are increasingly concerned about policies that are honoured in the breach. We can talk about the privacy impact assessment policy, PIA. We continuously find that programs that have significant consequences for personal information protection go ahead without a privacy impact assessment. That was the case of the recent do-not-call list put on by the CRTC. That's an obvious one to do a privacy impact assessment on, but it's being done now, after the program has been in force for about a year.

One of the audits that my office did was to see how departments comply with the policy of having to do an annual privacy report. The answer is that they do a kind of so-so job, because it's not seen as something that is essential enough. So I think the distinction between policy and law is an important one, and certainly laws get the attention of a large and busy bureaucracy better than policies.

Mr. Bill Siksay: In the next paragraph, there's a list of a number of new policies that are in development at the Treasury Board Secretariat. I'm wondering if you're in consultation on the development of any of that policy.

Ms. Jennifer Stoddart: Perhaps I could ask my colleague, because she's actually talking to Treasury Board.

Ms. Chantal Bernier: Yes, we have regular meetings with them, and indeed, we are working with them on these. We have commented and we have been involved.

● (0945)

Mr. Bill Siksay: Terrific.

In the next paragraph—I've lost track of my numbers here, I think it's the eighth one—there's a line that says, “Law enforcement and security agencies cannot operate in silos and must be able to share intelligence quickly and efficiently.” This is in response to a concern that concerns about privacy really aren't well placed in terms of issues of law enforcement and security. Can you comment on whether or not it's possible to have privacy requirements that are efficient and don't block the transfer of necessary data between law enforcement agencies?

Ms. Jennifer Stoddart: Again, I'll ask my colleague to comment because of her knowledge of national security.

Ms. Chantal Bernier: I would go even further than that. I would put to you that greater discipline with respect to privacy will bring greater effectiveness in public safety measures. I would simply give you the example that being disciplined but collecting only relevant personal information will mean that you will have only information that you truly need for your public safety need, and you, at the same time, adopt a minimalist approach, which is the foundation of collecting personal information.

As you may have noticed, the key message was stated by the commissioner in her opening statement of our annual Privacy Act report. We feel that privacy and security go hand in hand. They are not at odds. We can give several examples of how, indeed, the protection of privacy helps discipline and streamline the public safety national security processes, thereby contributing to their effectiveness in addition to respecting fundamental rights.

The Chair: I want to move on. You are on the second round, Mr. Siksay.

We'll go to Madam Davidson, please.

Mrs. Patricia Davidson (Sarnia—Lambton, CPC): Thank you very much, Mr. Chair, and thank you very much, Ms. Stoddart and Ms. Bernier, for being with us today.

I certainly enjoyed reading your annual report. Thank you for that and for the work you're doing through your offices. I think it's an extremely important role. Certainly, Canadians need to feel comfortable that their privacy is being protected, so it's very important that we have these updates and so on.

I'm going to refer to page 1 of your report. You state that the "... report explores two of the most serious threats to privacy today. In two often intertwined themes, we report on the urgent need to integrate privacy protections into state security measures, and on the impact of information and communications technologies on the privacy of individuals."

Could you explain to us what the privacy impact assessment process is? How do you determine that?

Ms. Jennifer Stoddart: We ask departments or agencies to look at every step in their proposed program or the proposed measures in the light of the Privacy Act as well as what we call the fair information principles. It has been said to us that strictly speaking these aren't part of the Privacy Act, and that's true, but these are the modern iterations of good data protection standards in the light of their impact on individuals' privacy in terms of keeping the personal information private.

We then look at the assessments that were done. We dialogue with the departments. We make suggestions. We point out where there could be changes. Sometimes the departments will make changes and sometimes they won't.

That's basically the process.

Mrs. Patricia Davidson: Thank you.

Also in your report, you talk about Canada and its role in the global sector. I take from what's in here that we are a leader in the world in privacy issues. Can you tell us about the international organizations you're a part of and the leadership role you and Canada take in these organizations to help our international friends and allies in terms of privacy issues? In particular, I know you've referred to the Asia-Pacific area and the Francophonie areas, so tell us a little bit more about those initiatives, please.

Ms. Jennifer Stoddart: Starting with the Francophonie and the Asia-Pacific area, perhaps?

Mrs. Patricia Davidson: Sure.

Ms. Jennifer Stoddart: I'll start with the Asia-Pacific, and then maybe my colleague can continue with the Francophonie, and then we can come back to the others.

Asia Pacific Privacy Authorities, or APPA, was started by New Zealand, Australia, and Hong Kong, who have similar world standard legislation, to try to get some momentum going in terms of data protection in that area of the world. They have meetings about three times a year, and they share programs and they educate and they discuss how they deal with certain similar issues. Working meetings at APPA are very focused.

A couple of years ago, my B.C. colleague, Commissioner Loukidelis, and I were asked to join. We said yes, Canada is a Pacific nation, and increasingly we're looking toward the Pacific. I'd say we attend the meetings irregularly because of the cost and the time involved, but we have regular phone conversations with APPA and we communicate by e-mail on similar issues quite a bit, so there's quite a good rapport. We had a common youth privacy campaign together, where we took a video that had been made in Hong Kong and put it on our website and promoted it in Canada.

So that's APPA.

● (0950)

Ms. Chantal Bernier: La Francophonie association of data protection authorities is a subsection of the great Francophonie organization. It brings together, therefore, the authorities for data protection of the members of the Francophonie. The purpose is truly to provide us with a comparative basis, learn from each other, and enrich each other's work and policies in sharing experience.

Some of the main activities of the last year are the following. We have produced a report on what we've called the Canadian model—Quebec, New Brunswick, as well as the federal model—and it has been distributed widely through universities, through Francophonie data protection agencies and so on, to show how a governance structure for the protection of privacy can work well and enhance and help states that are still developing those structures to do so.

We have also contributed, just two weeks ago, to a whole seminar of the Francophonie, where we specifically addressed the issue of protecting data in a globalized world. In doing so, again, we shared our good practices with others and learned about the Francophonie states' good practices. All of us are getting better together.

These are the main activities under the Francophonie for this last year.

Mrs. Patricia Davidson: Thank you.

Ms. Stoddart, in your opening remarks to us you talked about the closing of complaints files and the backlog you've been addressing. You indicated that you were able to close almost 13% more this year than in the previous year and you are on track to eliminate this backlog altogether by next March. Could you tell us a little bit more about that process? What has enabled you to make this remarkable progress?

Ms. Jennifer Stoddart: We've actually been planning it for several years. At first, I guess progress was slow. I know that we've often been before this committee on this issue. But finally, all the things we were working on seemed to come together. We've kind of had liftoff, as you would say.

What have we done? First of all, we had an intense recruitment campaign. Our HR issues have been critical in the past. We're now fully staffed. We have extensive training for new investigators and for other employees. We have completely redone the technological infrastructure for case handling. We have just put it in place to help track, identify, and deal with the different cases a lot better.

We have looked at investing in upfront advice and help for Canadians. We're increasingly saying that when Canadians come to our office, they want help, they want information; they don't necessarily want a complaint that is going to drag on for umpteen months. Increasingly we're trying to say that we'll send a letter, we'll let people talk to somebody, and we'll give them the tools so they can go away and try to solve this. We're trying to reduce the number of requests for help that turn into formal complaints, because as we know, the Privacy Act is not one that leads you to any huge solution at the Federal Court anyway, so it's better to get these problems solved up front.

I think it is a combination of those things.

● (0955)

The Chair: Thank you.

Madam Simson, you can start the second round.

Mrs. Michelle Simson: Thank you, Chair.

To go a little bit further with the complaints section of your report, Ms. Stoddart, 546 of the 748 complaints received by your office relate specifically to access to information and/or timely compliance by various departments in providing information to inquirers. Do you have a year-over-year figure, such as the number in 2007 vis-à-vis 2008? I'm trying to determine whether it's getting better or worse.

I would appear to me, because this committee is also looking at access to information, that we're looking at two ancient pieces of legislation—they are a quarter of a century old—that seem to be overlapping and creating more work for you by virtue of the fact that the Access to Information Act hasn't been updated and properly enforced.

I was curious to see if we're going forward or falling backwards.

Ms. Jennifer Stoddart: I have a five-year overview of complaints, but I don't have the ones particularly on access. What I can say is that traditionally and constantly, people come to us for access to their files or because of issues of access to all the information they believe is in the files. They don't agree with the exemptions, or they think there's something more, or the departments have taken more than 30 days to respond. That's kind of the constant best seller in our work.

Mrs. Michelle Simson: In other words, if the government were able to update these antiquated acts, there is a good chance, with respect to timely compliance and access, that you could considerably cut down on the workload with respect to complaints in your office.

Ms. Jennifer Stoddart: I think one of the things that could help this particular issue of delay, and this is for the Privacy Act rather than the Access to Information Act, would be investment in what are called the ATIP units. They're often overwhelmed. It's not seen as being as important a function as other ones. They're often chronically understaffed. It's a very lonely job to be there and to give out information that may be controversial for your colleagues and so on.

For example, we have a huge number from the Correctional Service of Canada. The largest single number of our complaints come from the Correctional Service of Canada.

Mrs. Michelle Simson: Would that be basically from people who are incarcerated?

Ms. Jennifer Stoddart: That's right, and that has always been the case since I've been Privacy Commissioner. We're trying to work with them systemically, and I know they have invested more in their ATIP resources, with the result that we have fewer complaints that are taking more than 30 days.

Mrs. Michelle Simson: Thank you.

Mr. Borys Wrzesnewskyj: I understand the RCMP continues to be one of the biggest generators of complaints. I don't have a lot of patience with complaints generated by those convicted of criminal activities. But it's the other types of complaints that worry me. In the past, there were frequent allegations that the RCMP was gathering information in excess of what is allowed or required. They have eliminated some of their so-called exempt databases or diminished their use.

Have you had an opportunity to look into allegations made by actual RCMP officers who work, for instance, in the ATIP section? We have heard allegations of misfilings, allegations that some files were designated “secret” when they shouldn't have been. Retired officer Estabrooks made similar allegations in another committee when he was being questioned a couple of years ago.

Have we actually gone in and talked with some of these retired RCMP officers who have made these serious allegations of gathering unauthorized information and of files disappearing or being misfiled?

● (1000)

Ms. Jennifer Stoddart: I know you are concerned about that. I don't think we have looked into that issue on a systemic basis. But perhaps my colleague, who is closer to the files, can answer.

Ms. Chantal Bernier: Yes, the operative word is “systemic”. We have received some complaints by RCMP officers who were concerned about the way some information had been dealt with. We investigated and made a finding, but as the commissioner said, we have not done a systemic review.

The Chair: Thank you.

Mr. Dechert, please.

Mr. Bob Dechert (Mississauga—Erindale, CPC): Thank you, Mr. Chair. Good morning, Ms. Stoddart and Ms. Bernier. Thank you for your report and for your remarks here today.

Our government's top priority is the safety and security of all Canadians. You mentioned something about this in your report. Can you tell us how you are working with Citizenship and Immigration and the Department of Public Safety to ensure an appropriate balance between privacy, efficiency, and security in preparation for the 2010 Olympics? Maybe you could also comment on the G8 and G20 conferences that are coming up next year, with respect to visitors to Canada.

Ms. Jennifer Stoddart: I'll begin and then I'll refer it to my colleague. She has a background in national security and is in charge of this file.

We started almost a year ago because of the concern that we heard from citizens and from our colleague the B.C. commissioner. We have been working quite assiduously, and we now have on our website a joint section with the B.C. commissioner that goes into quite a bit of detail on the security issues at the Olympics—what people can expect, where they can make complaints, what is legal, what rules should apply to security and privacy situations.

Chantal can give more details.

Ms. Chantal Bernier: As the commissioner said, we have followed this assiduously. Starting in February of this year, we have sent to the Integrated Security Unit a list of questions to hold them accountable for protecting privacy during their public safety measures. We have received a briefing from them in Vancouver. They have answered every one of our questions satisfactorily, and they have also implemented our recommendation that they appoint a chief privacy officer to oversee, from within, the safeguards that they apply.

In addition, I must say that I have been satisfied with my relationship with the head of ISU, who has been very forthcoming. When I do hear of concerns—we see from the media there are concerns raised by citizens—I have been able to speak to him and address every one of our issues. In addition, the joint website that we have with the B.C. privacy commissioner allows Canadians quick access to what they should know about ensuring that their privacy is respected during the games.

Mr. Bob Dechert: It sounds as though there's good cooperation, then, between your office and the authorities responsible for securing our safety during these very important games, which are a source of great national pride, but obviously we're concerned about keeping our country safe at the same time. Thanks very much for that.

In your remarks this morning, Ms. Stoddart, you mentioned the very good progress you've made in reducing the number of complaint backlogs. I have a couple of questions.

You mentioned that you had redefined what constitutes a backlog. Perhaps you could give us a little more explanation on that. That had the effect of increasing the number of cases that you would then describe as being backlogged. You then substantially reduced them, which is good to see. You mentioned earlier, in answer to one of the other questions, that you'd done a five-year overview of complaints and backlogs. I wonder if you could take us through that five-year history.

Ms. Jennifer Stoddart: In answer to the first part of your question, honourable member, with hindsight it seems to be the obvious thing to do—that's why there's hindsight, I guess. Traditionally we'd said that the backlogged complaints were the complaints not assigned, but as we struggled on through various administrative challenges and we had this increasing number of files that we couldn't get to, we thought, why not be really transparent and strict with ourselves and take the standard that's in our other law and say that complaints should be serviced within a year, maximum? So everything that has been in our files for over a year is, by definition, a backlog, whether somebody's working on it or not.

● (1005)

Mr. Bob Dechert: What was the previous standard?

Ms. Jennifer Stoddart: The previous standard was that the file was unassigned. You could assign files and then the parties could be talking sometimes for years. That wouldn't be in a backlog.

I'm happy with this new standard. It's a clear, objective standard. But one of the things that happened then was that a lot of files that previously weren't defined as backlogged went into the backlog, and then we had administrative challenges, and so on. So things got a lot worse before they will get better, which is why our present figures are not great. The good news is—I am sure, and I have asked—that by the end of March all files that we've had for over a year will have been dealt with under the Privacy Act.

The Chair: Do you have one quick question?

Mr. Bob Dechert: I want to ask you about your comment, on page 3 of your remarks this morning, about our relations with foreign intelligence partners and sharing of information. Can you describe how Canada's system compares to some of those foreign intelligence partners?

Ms. Jennifer Stoddart: Honestly, honourable member, no, I can't. Traditionally, as you know, in the last few years this has been a challenge. We've said that when it's not done precisely and carefully there can be huge human consequences. Some of our preoccupations in the recent FINTRAC audit were that somebody could get into an unsubstantiated database and make a decision based on that when in fact the evidence isn't there to back it up. It's a general concern.

Mr. Bob Dechert: Would it be possible for you to report back to us on what happens in the U.S.?

The Chair: Thank you, Mr. Dechert.

[*Translation*]

Mr. Dorion, you now have the floor.

Mr. Jean Dorion (Longueuil—Pierre-Boucher, BQ): Thank you, Mr. Chairman.

Madam Commissioner and Madam Assistant Commissioner, welcome to this committee.

Ms. Stoddart, thank you for the political independence your report exemplifies. You do not hesitate to say, among other things, that you were disappointed by the government's refusal to reform the Privacy Act.

Our committee received—I expect that you were informed of this—a response from the Honourable Rob Nicholson, Minister of Justice, to a report we had submitted to the government. The minister entitled that response: "Government response: tenth report of the Standing Committee on Access to Information, Privacy and Ethics [...]". Our report was tabled in the House of Commons on June 12, 2009.

In his response, the minister refers to the fact that in our report, we made five recommendations that you had yourself submitted and which were included in the 12 recommendations in your own report. More particularly, the minister said that we had chosen 5 of the 12 recommendations you made.

Are you of the opinion that this committee's report defended your positions well?

Among your own recommendations, are there any you would have liked the committee to give greater attention to?

Ms. Jennifer Stoddart: Thank you for your questions.

Of course, I would have liked to have seen the committee endorse our 12 recommendations without hesitation. However, I'm very happy with this report because first of all, it is the most serious review of this act that has been carried out in 20 years. Indeed there was a long period of time that elapsed during which there was no review. So this is a very serious review. Secondly, I'm very happy with the fact that this committee was able to unanimously endorse about half of my recommendations. As for the others, I don't think they were just rejected out of hand. It could have been that they concerned very complex issues. I note the fact that further studies were suggested.

● (1010)

Mr. Jean Dorion: Were certain aspects not chosen that you would have liked to have seen in the report?

Ms. Jennifer Stoddart: You are talking about aspects concerning which you had recommended further studies?

For instance, on the matter of the processing of complaints and recommendation No. 6, where you suggested that I be given the discretionary power of discontinuing or refusing to process certain complaints, I would have liked to see the committee support that recommendation unanimously. In fact, I hope that I will be able to obtain this power in the act with regard to the private sector. And thus, if I can do this for complaints that come from the public concerning a business, it seems to me that I could also do so in the case of complaints against the government, its departments and agencies.

And don't forget that if I make a mistake, the Federal Court can let me know and bring me back into line.

Mr. Jean Dorion: In this year's report, we can see on page 82 that 187 complaints out of 990 were discontinued, and that 121 of these concerned access and 38 concerned use and disclosure. As citizens, we know that it can be very frustrating to file complaints and to see that treatment times may be very long, to suspect that there may be ill will on the part of people who are following up on complaints or dragging their feet, and so forth.

What, in your opinion, is behind the discontinued complaints? Perhaps there is less of a tendency to study complaints that were discontinued rather than the ones that were maintained. Do you have an explanation as to why people file complaints and then withdraw them?

Ms. Jennifer Stoddart: There are probably several reasons. In order to have a better idea, we would have to do a cross-check with the nature of the complaint. Sometimes people have unrealistic or inaccurate expectations with regard to what we can do or what we can obtain for them. I'm thinking in particular of people who believe, because they watch a lot of American television, that if they turn to us, we will be able to sue the government and obtain compensation for them. But we cannot do that. And so they get discouraged or feel that it is not worth going forward.

There are also processing times to be considered. We are living in an era where a simple click of a mouse can cause things to happen. And so, the fact that the process is slow—which is one of my concerns, and I don't hesitate to say so—is certainly a factor.

[*English*]

The Chair: They do happen. They do, and sometimes they're not the right things either.

Mr. Poilievre, please.

Mr. Pierre Poilievre (Nepean—Carleton, CPC): Thank you.

My questions pertain to the modern technological environment in which our privacy laws operate. There have been high-profile discussions about privacy issues related to both Google and Facebook in the last several months, discussions that I think in Canada have been very positive, starting with Facebook.

You and your office are credited with having done some good work with Facebook to establish norms of data retention and policies for the deceased who had Facebook profiles. To Facebook's credit, it has been very responsive to that discussion, and it has come forward with some very innovative and positive solutions to those privacy problems. In Google's case, their Street View technology has been adapted to meet the requirements that exist in our commercial privacy legislation. Both of these companies, I think, deserve some commendation for very innovative, prompt responses to the demands of privacy advocates and your office.

Do you believe that current laws equip us to deal with modern technological innovations like Google and Facebook? Or do you believe the transformation of our technological landscape requires that we update our laws?

● (1015)

Ms. Jennifer Stoddart: I'd say that as a matter of principle we should constantly be looking at updating our laws in terms of the... you don't know what adjective to use because the pace of change is so enormous in terms of communication technologies now. That is the role of those who look mostly at our private sector law.

In fact, there are some changes to it going through now. The government, I'm very happy to say, has introduced anti-spam legislation. That's a huge improvement. Also, PIPEDA is reviewed every five years, which is something that we've asked for in regard to this law, and I believe that's one of the things the committee endorsed.

So yes, as a matter of principle, we constantly have to look at this. Data breach is a huge problem. A lot of our report deals with data breaches in the government, and of course we know that outside of the government it's a huge problem.

Mr. Pierre Poilievre: That's great, but you seem to have had some success with both of these companies using the existing statutes and the existing rules. Do you believe that the laws perhaps establish certain principles that can transcend the changes in the privacy marketplace, or do you believe we are ill-equipped to deal with those changes?

Ms. Jennifer Stoddart: No. I think our dealings with those two companies show the basic solidity of the Canadian law. One of the honourable members talked about Canada's role internationally. It's largely because there's huge interest in our law being a law with very high standards, but a flexible and practical application, one that can be adapted to different situations. I think the basic principles in the law are very sound. Our challenge is to adapt them.

I'd add one caveat, though. It is a consent-based law. Some of the discussion in international conferences now is about what consent is worth when we just click on to get to the next screen and click on “I consent”. None of us reads this. Even if we do read it and we are lawyers, we don't know what it means. As for how to have it enforced, if it were enforced, it would be two years from now anyway, so we just click on.

That is increasingly an issue. Should we go to another form of participation or should we make clear standards for some of these companies because the consent in legal terms is not meaningful? That is one of the ongoing debates, but for the moment, we've been able to adapt our law to the challenges.

The Chair: Thank you.

I have Mr. Siksay, followed by Madam Block.

Mr. Bill Siksay: Thank you, Chair.

I want to come back to the questions around privacy and the Olympics. I appreciate that you've had good cooperation from the ISU and the head of the ISU, Mr. Mercer. That was my impression as well, when I met with him on security issues related to the Olympics.

I wonder if there will be any monitoring or process in place to deal with any privacy complaints that arise during the course of the games. Is there going to be an examination after the games of what happened with regard to privacy concerns throughout the whole process of planning and operation of the games?

● (1020)

Ms. Jennifer Stoddart: Yes, we have discussed that with David Loukidelis.

I'll let Chantal Bernier answer. She's the one who is on this.

Ms. Chantal Bernier: The chief privacy officer who has been appointed would be the first line to receive any complaints, but our process would apply as well. Therefore, we would entertain any complaints that could occur.

At this point of course, we are trying to instill safeguards in the whole process. But hopefully we'll avoid that....

Mr. Bill Siksay: Is there a plan to do an overall review of what happened with regard to privacy in the Olympics when the games are over?

Ms. Chantal Bernier: At this point no, unless you see that as being the conversations we have with the ISU. We are making sure we apply this review now. As I said, we sent them the questions we felt were relevant to hold them accountable in advance. We stated all the things we felt they should do, including training, appointing a chief privacy officer and so on.

We feel at this point that things are being so well handled that there may be no need for further intervention.

Mr. Bill Siksay: With regard to large international events like the G8 and the G20 meetings, has there ever been...audit is probably the wrong word, but an audit of privacy concerns around those kinds of major international events?

Ms. Chantal Bernier: Not that I know of. I can tell you that in preparation for our holding the ISU accountable we have spoken to foreign counterparts who have been the data protection authorities at the time of Olympic Games. We have also looked at literature, research, on experiences around large events. There are academics who have looked at that specifically, and we have informed ourselves of their findings. In a nutshell, there are obviously unique situations where the imperatives of public safety are so great that they call for certain enhanced measures, which at the same time call for greater alertness towards privacy and an adaptation to the context.

Mr. Bill Siksay: Have you been involved in the planning for the G8 or G20 meetings in Huntsville, Ontario?

Ms. Chantal Bernier: No, not yet.

Mr. Bill Siksay: Commissioner, in your press conference the other day, I believe you said something about being disappointed that there hasn't been an overall security review—I could be wrong, so clarify this for me—and that a group of commissioners has recommended such a review. Am I on the right track? Can you explain what you were commenting on?

Ms. Jennifer Stoddart: You're talking about my comments on the no-fly list, the passenger protection program.

Mr. Bill Siksay: I'm not sure if it was just the no-fly list or if it was an overall review of security measures and how they had rolled out over the years.

Ms. Jennifer Stoddart: I think those comments were related to the no-fly list and the extensive concerns we advanced in the summer of 2007 when this was first rolled out. My office and the offices of the privacy commissioners across Canada unanimously adopted a resolution and, among other things, asked for oversight, some reporting, and a substantial parliamentary review. We asked for the development of specific regulations on which such a program would be based. It was those things that had not been developed and in which I expressed disappointment.

Mr. Bill Siksay: With regard to your specific audit of the no-fly list and Transport Canada in that regard, I think there were four issues: the sign-off by the deputy minister, the security of lists being used, breach reporting, and computer certification of the system used to hold the list. You said that Transport Canada had responded positively; I think that was the phrase you used. Can you explain what that means? Has it changed those processes? Does the deputy minister now get information before signing off? Is that done, or is it a work in progress?

Ms. Jennifer Stoddart: No, my understanding is that it was changed immediately, because it was—

Mr. Bill Siksay: In all cases?

Ms. Jennifer Stoddart: Yes, or it's in the process of being changed.

Could I just add this, Mr. Chairman, because I think the committee should know about this in terms of what we're doing with the Olympics. One file that did take a bit of time, and it took a trip to Brussels by me and the Quebec commissioner, was the European data protection authorities' concern—and particularly something called the article 29 working group, which speaks on privacy issues, data protection issues for the European Union—about the application of anti-doping standards at the Olympics. These are run out of something called WADA, the World Anti-Doping Agency, in Montreal. Canada has been very prominent in the fight against doping in sports, so both of us, my Quebec colleague and I, responded on how our different laws would apply. It is not impossible that this issue will come up again during the course of the Olympics, and we are, with the B.C. commissioner, prepared to respond to it then.

● (1025)

The Chair: Thank you.

Madam Block, please.

Mrs. Kelly Block (Saskatoon—Rosetown—Biggar, CPC): Thank you very much, Mr. Chair, and welcome to Ms. Stoddart and Ms. Bernier.

I would like to take us back to your report and ask some questions around FINTRAC. I read in your report regarding FINTRAC and the fact that it's an independent agency with a mandate to collect and analyze financial transactions for the purpose of monitoring suspicious financial transactions that may relate to terrorism or organized crime. While they have always worked to balance security and proximity, can you tell us about the positive changes that FINTRAC has made in response to your report?

Ms. Jennifer Stoddart: Yes. We say that they responded to 10 out of 11 reports. I couldn't rhyme them off by heart, but what we did is publish as a separate publication this time—this is new—the complete original report rather than just giving highlights, because we thought it would interest the public. In fact, it is interesting reading. Many of the suggestions FINTRAC changed right away. We're very happy that with regard to our main problem, which is the storing of unverified and indeed unsubstantiated information with information that is of adequate quality, they are taking steps to go through all that information and sort out that information that should not be in their data banks.

Mrs. Kelly Block: I note that the amendments that were passed in 2006 would give your office the authority to review FINTRAC every two years. Is this the first review that you've conducted since those amendments were made?

Ms. Jennifer Stoddart: It is. It's the first time we've done an audit on FINTRAC according to our statutory mandate, so we'll be back to follow up in two years.

Mrs. Kelly Block: Thank you.

The Chair: Madame Faille, please.

[*Translation*]

Ms. Meili Faille: My question concerns information technology. On page 43 of your report, you state: “[...] it is clear that future trends in computing will only magnify and intensify the risks”. Have you, in exercising your mandate, had the opportunity to examine the government plan to enhance these technologies, among others the project to modernize the federal government's technological infrastructure?

On page 44, you say that the Canadian public is demanding access to ever more services over the Internet. One project that is known as the “secret channel” will be abandoned. New technologies are going to be used. The call for tenders in connection with those technologies should be out in two weeks. I was wondering if during the past three years, you had been consulted concerning these technologies the government intends to use.

Moreover, within the framework of this modernization plan, questions have been raised by Canadian businesses and citizens concerning the storing of data in databases located throughout the world because of call centres. The government is increasingly choosing large Internet providers. Call centres and databases are thus managed elsewhere. In the case of Bell Canada, we know that this takes place in India. How are we going to protect these data and who will have access to them? How are we going to ensure that this information is secure? Would you be willing to help us and to provide us with comments and recommendations on this?

You seemed a bit surprised a little earlier, but I am asking you this question because of the speed at which things are developing at this time. The replies obtained at the Standing Committee on Public Accounts indicate that the network is slowing down to some extent. Questions were put concerning the Access to Information Act and Privacy Act. A committee report which concerns your interests will be tabled in the near future.

Can you tell me if your office has had an opportunity to assess the government's program to modernize its technological infrastructure? That project comprises four pillars.

● (1030)

Ms. Jennifer Stoddart: I don't think there was an official review of one or the other of those pillars. We have computer experts and we are about to hire more of them. The government consults them on a voluntary basis. If we have not been invited to participate in the process, we won't be contributing to it. I think that we will only be peripherally involved.

Ms. Meili Faille: You are carrying out a study at this time. Could this matter interest you? The government will be choosing its supplier very soon. We are talking here about replacing 144 federal government computer systems. This concerns all of government. Would it be opportune for you to intervene quickly for the reasons you mention in your report?

Ms. Jennifer Stoddart: I take good note of your questions. They are very important.

We are indeed assessing the implications that this government wireless network will have on privacy. I would also remind you that under Treasury Board policy, and not the act, the government itself should assess the factors that may have repercussions on privacy and submit the results of that assessment to us before making a definite commitment. That is what the policy requires, but as I have already said, it is often set aside. That is why we asked that similar cases be covered by provisions in the law.

Ms. Meili Faille: Yes, I agree with you. A policy is a policy and the government is not respecting it. The Auditor General said that she had the same concerns. She would like assessments to be made before such projects are implemented or go forward and before funds are allocated to them.

Certain technologies that are not really new, for instance the famous BlackBerrys, have an impact on privacy. Would it be possible to give us guidelines on federal government surveillance of PIN to PIN communications involving BlackBerrys? Can an employer have access to them? Can non-authorized and unjustified communications that took place using BlackBerrys be reconstituted? Could this be used for administrative investigations into frauds?

Ms. Jennifer Stoddart: I am taking good note of this.

Ms. Meili Faille: Thank you.

[*English*]

The Chair: Mr. Rajotte, *s'il vous plaît.*

Mr. James Rajotte (Edmonton—Leduc, CPC): Thank you very much, Mr. Chair.

Good morning. Thank you for being with us here. It's good to see you again, Ms. Stoddart. It's good to see you, Ms. Bernier.

I did want to follow up on FINTRAC and I also wanted to talk about your recommendations for Transport Canada. You made four recommendations to Transport Canada. My understanding is that they were responding to two of them perhaps before the report is even published, and the government has indicated that it's working on the remaining two recommendations.

Could you provide an update on those two recommendations?

Ms. Jennifer Stoddart: Yes. I believe I don't have much to say, honourable member, because we are quite pleased with the cooperation on these recommendations and the follow-up that is going to take place. Our concerns remain with the overall operation of the program and the fact that Canadians don't have an idea of who is on the list, how they get on exactly, and do they ever get off. I was asked many questions about that. That's not in my mandate. Transparency would be appreciated in this.

● (1035)

Mr. James Rajotte: In terms of the four recommendations, you're satisfied with this?

Ms. Jennifer Stoddart: Yes, we are.

Mr. James Rajotte: Thank you very much for that.

I wanted to follow up on Ms. Block's questions on FINTRAC. You mention in your opening statement and one of your key recommendations is that FINTRAC "do more work with reporting organizations to ensure it does not acquire personal data beyond its mandate". Then in your FINTRAC report, which I appreciate and I'm glad you did release it in full, you said, "the Centre acquires information in two ways: it receives and collects it. While we found no evidence to suggest FINTRAC is collecting information beyond what is authorized, we noted that it has received and retains information beyond the Centre's legislative authority". I think that's a very important distinction in terms of receiving and collecting. So it's not exceeding its mandate in terms of collecting but receiving.

You also talk about working with organizations. Later in the report you mention...I think the example was the casino forwarding information to FINTRAC. Is the problem that FINTRAC is receiving information they're perhaps unaware of or they're not following it exactly? They should report to the casino right away. If it's under $10,000 they're not entitled to receive this and provide the full stop at that point. Is that—

Ms. Jennifer Stoddart: That's absolutely it, honourable member.

Mr. James Rajotte: Are you satisfied with FINTRAC in terms of their response on that recommendation in the sense of following that procedure now, whereby they will be providing a stop and they will not be receiving information they're not entitled to?

Ms. Jennifer Stoddart: Yes. FINTRAC was very cooperative. They have a very difficult task to do. Cooperating with that recommendation to pre-screen the information before putting it in the bank is going to be onerous for them, but they are committed to their best efforts.

Mr. James Rajotte: I certainly appreciate that.

In your annual report on page 31 you talk about the destruction plan: "The Centre is developing a strategy to move forward with a destruction plan." This is information that either they should not have or perhaps they can receive but they should have a plan in place to not retain that information. Obviously, if it's a paper copy, you can shred it and it's very simple. As you all know, and as we've discussed on previous occasions, when it's electronic, as my friends in the IT sector say, it's almost impossible these days to destroy something.

Can you comment on a destruction plan, especially with respect to information that is held electronically?

Ms. Jennifer Stoddart: Honestly, honourable member, I can't. I don't have that level of knowledge. I understand that is the challenge before FINTRAC. That is why they didn't say they'd do it tomorrow. They said, yes, they would use their best efforts. I gather to delete the information that's extraneous to their mandate at this point is a complex and demanding process, because the information is on a huge number of files stored electronically. What's important is that they are going to try in good faith to comply.

Mr. James Rajotte: A lot of your good work is referenced not only in the public sector but in the private sector, and this seems to be one of the main challenges for privacy commissioners and for countries going forward: how to ensure that information obtained and stored electronically is not stored past a certain point. Is there something for this committee's information? Who is responsible for ensuring that information that was acquired is no longer there?

Ms. Jennifer Stoddart: Well, it's the holder of the information, according to the laws that apply to it.

But you're right: throughout the world this is a huge problem. It's so easy to collect the information. It may be wrong and it may be irrelevant, but it is collected, and then how do we get rid of it and how do we delete it? It's an increasing challenge for all of us.

Mr. James Rajotte: I appreciate that very much.

The Chair: Thank you, Mr. Rajotte, chair of the finance committee, for bringing some continuity to an important area of discussion. Thank you for the questions.

Finally, we'll have a brief question from Mr. Siksay.

Mr. Bill Siksay: Thank you, Chair.

I want to come back to your comments on the biometrics introduction that CIC is planning. This is a two-part question.

Has CIC done a privacy impact assessment on your biometrics program? As well, the whole question of transferring fingerprints of refugees to other jurisdictions sets off all kinds of alarm bells for me, given that refugee claimants have often been persecuted in their country of origin. If we don't find that they're legitimate refugees, there may be real concerns for their security in their country of origin. I wonder if you could comment or expand on that a little more.

● (1040)

Ms. Jennifer Stoddart: Yes. Chantal is familiar with this program.

Ms. Chantal Bernier: I would say that your concerns are exactly ours. We are working with CIC precisely to address all of those issues. They are doing a PIA. We are working with them in reviewing that.

Mr. Bill Siksay: Thank you.

Thank you, Chair.

The Chair: Madam Stoddart and Madam Bernier, this has been a very comprehensive review of many of the issues that have gone on. I want to thank you very kindly for assisting the committee in better appreciating some of the challenges we face. I certainly thank you for the annual report and the special reports, particularly on matters like money laundering, FINTRAC, Facebook, Google Street View, and the list goes on.

We will never finish. As a consequence, I want to invite you to continue to work with the committee and, more specifically, to suggest next steps. Undoubtedly, we will be having a steering committee meeting before the Christmas break to consider suggested work in the areas under our mandate. We want to build on where we've been. We want to make sure the prioritization is right.

As you know, these processes, even what we've gone through, take a fair bit of time. The sooner we identify those priorities, the sooner we make a commitment to them and start to plan. We will hopefully have the time of the Christmas break to formalize a process so that when we come back in January we will be able to proceed right off the bat.

We certainly welcome your thoughts, suggestions, and input on either the completion of matters that have already been addressed but may require some additional work or, indeed, on moving us to a new horizon that may be an emerging issue.

I thank you. I understand that you have other things to do, and we have another matter, so you're excused.

Ms. Jennifer Stoddart: Thank you, Mr. Chairman.

May I say on behalf of all my staff how much we appreciate the interest and support of this committee in our work? As an agent of Parliament, you're kind of alone. You don't have a minister and you're not a department. The fact that the committee takes such an active interest in our work and provides us a sounding board is very useful.

Thank you.

[*Translation*]

Ms. Chantal Bernier: Thank you.

[*English*]

The Chair: Thank you.

I don't think I'm going to suspend. I would like to go on to our other matter of business, which is the consideration of the government response to the tenth report, on the privacy quick fixes.

We did receive a letter from the minister, and that was previously circulated. There are copies available and I think those are being circulated again, just for the members' information.

For the members' recollection, in regard to the privacy, this is a project that actually started in the prior Parliament, and the committee, after the last election, adopted a motion to bring that matter forward to the current Parliament. We have had the minister this Parliament for one hour—that's it—and his correspondence.

Our report and our work were substantive, I think. And as was indicated in the dialogue with the Privacy Commissioner, there is a clear understanding that we were not in total agreement with all of the so-called quick fixes. We did embrace five, or possibly six. I think it's fair to characterize the others as maybe either premature or that we need more work on some of those. So we'll have an opportunity to consider those, if necessary, when we do continuing work.

I think we will want to consider in a steering committee meeting, which likely will be held next week, whether there is any further work. So I would ask the members to refresh themselves on that.

We do have a call for a vote in half an hour. Normally when a vote is called, the committee should not be meeting without the unanimous consent of the committee. Could I have an indication from the members whether or not they would like to proceed for a short while, or shall we adjourn?

● (1045)

Mr. Bob Dechert: Mr. Chair, if I may, our whip has asked us to proceed to the House as soon as possible.

The Chair: All right. Those are the rules. We will pick this matter up at our next meeting next Tuesday. I hope the members will start to consider matters that may be dealt with at a future steering committee meeting.

We haven't been advised yet with regard to whether or not there will be a nomination of an information commissioner. That will be coming before us, with the nominee. And the estimates we still are determining; that may not happen until after the Christmas break.

I'm going to do my best to keep you informed. Please have your staff make sure you are advised as to the specific agenda for next Tuesday's meeting. But the first item will be this carry-over item.

Thank you kindly.

We're adjourned.

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

SPEAKER'S PERMISSION

Additional copies may be obtained from: Publishing and Depository Services
Public Works and Government Services Canada
Ottawa, Ontario K1A 0S5
Telephone: 613-941-5995 or 1-800-635-7943
Fax: 613-954-5779 or 1-800-565-7757
publications@tpsgc-pwgsc.gc.ca
http://publications.gc.ca

Also available on the Parliament of Canada Web Site at the following address: http://www.parl.gc.ca

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

PERMISSION DU PRÉSIDENT

On peut obtenir des copies supplémentaires en écrivant à : Les Éditions et Services de dépôt
Travaux publics et Services gouvernementaux Canada
Ottawa (Ontario) K1A 0S5
Téléphone : 613-941-5995 ou 1-800-635-7943
Télécopieur : 613-954-5779 ou 1-800-565-7757
publications@tpsgc-pwgsc.gc.ca
http://publications.gc.ca

Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante : http://www.parl.gc.ca