House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 025 • 3rd SESSION • 40th PARLIAMENT

EVIDENCE

Tuesday, October 19, 2010

Chair

The Honourable Shawn Murphy

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, October 19, 2010

● (1530)

[*English*]

The Chair (Hon. Shawn Murphy (Charlottetown, Lib.)): I will now call the meeting to order.

I want to welcome everyone here.

Bienvenue à tous.

This meeting, colleagues, was called pursuant to the Standing Orders. On the agenda today, we're going to hear from the Office of the Privacy Commissioner of Canada in relation to the annual report of that office. The committee is very pleased to have with us Jennifer Stoddart, the Privacy Commissioner.

On behalf of all members of the committee, Ms. Stoddart, we want to thank you. I know that you've come before the committee on reasonably short notice and that you've had to rearrange your schedule, so for that we do want to thank you.

However, before hearing from Ms. Stoddart, I would like to deal with the minutes of the steering committee meeting held earlier today. Those minutes have been circulated. I will highlight them.

Basically, the minutes outline the recommended future business of the committee in dealing with the study on the street imaging application, the Google issue. There was a report, of course, issued by the Office of the Privacy Commissioner today, which I'm sure most members have not had an opportunity to read yet. The decision of the committee was to call back Google, invite back representatives from the Office of the Privacy Commissioner, and continue our discussion on the draft report on the study of street imaging, which is the same thing.

The decision was also to continue our discussion of possible committee reports. This is to deal with a report we did earlier on open government and proactive disclosure.

Last is a change to our routine motions. I'll read it:

> The committee recommends that a member (Liberal) be added to the subcommittee and that the routine motion be changed accordingly. It is understood that the chair will not vote in a tie at any subcommittee meetings.

Those are the minutes. The chair will entertain a motion for their acceptance.

Go ahead, Madame Freeman.

Mrs. Carole Freeman (Châteauguay—Saint-Constant, BQ): I'm sorry, but I didn't hear the motion.

The Chair: Okay. The chair would entertain a motion to accept the minutes of the steering committee.

Mrs. Patricia Davidson (Sarnia—Lambton, CPC): I have a comment.

The Chair: It has to be moved first.

Mr. Bill Siksay (Burnaby—Douglas, NDP): I'll move it.

The Chair: It is moved by Mr. Siksay. Is there any discussion?

Go ahead, Mrs. Davidson.

Mrs. Patricia Davidson: It was my understanding that the wording was that the chair would be a non-voting member of the steering committee, not that he would just not vote on a tie, but that he would be a non-voting member.

The Chair: But I will attend...?

Mrs. Patricia Davidson: Oh, absolutely. You're the chair.

The Chair: The chair will be a non-voting member. That's right. That's fine.

With that amendment, is there any other discussion? All in favour?

(Motion as amended agreed to—[See *Minutes of Proceedings*])

The Chair: Thank you very much.

We're now going to go back to the business at hand, and that is to hear from the Privacy Commissioner. She has circulated her opening comments.

I'm going to turn the floor over to you, Ms. Stoddart.

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

It's a pleasure to be back before this committee after the summer recess. I welcome this opportunity, because since I've last been before you, I have released two annual reports to Parliament. The topic for today is the findings in my two annual reports.

First of all, Mr. Chair, the annual report on the Personal Information Protection and Electronic Documents Act, known as PIPEDA, Canada's private sector privacy law, was tabled in June of this year. As you will also recall, Mr. Chair, we presented our most recent annual report to Parliament on the Privacy Act just two weeks ago.

Over the next few minutes, I propose to offer to the committee some highlights from those reports and some highlights of our work over the past year. Then I would be happy to take all the questions members of the committee may have.

First is the Privacy Act annual report. I will mention parenthetically for the new members of the committee that the Office of the Privacy Commissioner administers two privacy laws, one in the public sector and the other, the more recent, in the private sector. I'll start with the report on the one on the public sector, which is the one we released in September.

The Privacy Act report of September traced our efforts to safeguard privacy rights in the face of two key challenges: rapidly evolving information technologies and the pressures of national security and public safety measures. On the whole, it is safe to say that most public servants take good care of the personal information entrusted to them by Canadians.

Still, and unfortunately, there were some exceptions. One complaint to our office, for instance, involved the unauthorized access by Canada Revenue Agency employees to the tax records of prominent Canadian athletes. While such a breach cannot be undone, it did lead the Canada Revenue Agency to update its audit capabilities to better control access to personal information.

● (1535)

[*Translation*]

I now want to talk about wireless and disposal audits. The annual report also summarized two privacy audits we undertook during the year.

One found significant shortcomings in the way government institutions dispose of surplus computers, with many still containing sensitive data. We also discovered that documents are shredded by private contractors without the necessary degree of government oversight.

A second audit of the use of wireless networks and mobile devices of five federal departments and agencies uncovered numerous gaps in policies and practices that could put the personal information of Canadians at risk.

I will now move on to Veterans Affairs. Just a few weeks ago, we announced plans to conduct another privacy audit—this one of privacy policies and practices at the Veterans Affairs Department. This, as you know, was sparked by concerns that came to light during our investigation of a complaint launched by a veteran who has been an outspoken critic of the department.

Our investigation determined that the veteran's sensitive medical and personal information was shared—apparently with no controls—among department officials with no legitimate need to see it. The information then made its way into a ministerial briefing note about the individual's advocacy activities, something I deemed entirely inappropriate.

We are still working out the scope of the audit. We hope, though, that it will provide guidance as the department implements the recommendations stemming from our investigation.

In June, we also published our findings in an important audit on the private sector side. This one was triggered by a string of serious data breaches among Ontario mortgage brokers that compromised the personal information of thousands of Canadians. Our audit under PIPEDA found that the breaches caused several of the brokerages to take further steps to better protect personal information.

And yet, we determined they had not gone far enough. Indeed, our audit raised concerns about data security; the haphazard storage of documents containing personal information; inadequate consent by clients; and a general lack of accountability for privacy issues.

The audit was summarized in the PIPEDA annual report, which also highlighted the challenges of enforcing privacy rules in a world where data flows readily and instantly around the world.

● (1540)

[*English*]

I would like to talk now about Google Buzz and a bit of our international work.

We recognize that addressing this global challenge will demand agility and resourcefulness on the part of all privacy authorities. That is why, when Google disregarded privacy rights in the rollout of its Google Buzz social networking service last February, we opted for an innovative alternative to our conventional tools of audit and investigation.

Instead, we led nine other data protection authorities from around the world in an unprecedented—and I think highly effective—tactic: the joint publication of an open letter that urged Google and other technology titans entrusted with people's personal information to incorporate fundamental privacy principles directly into the design of new online services.

We are engaging with global partners in numerous other ways as well. Last month, for instance, we joined other data protection authorities from around the world to establish the Global Privacy Enforcement Network, which aims to bolster compliance with privacy laws through better cross-border cooperation. Later this month at an international conference of data protection privacy commissioners, I will be co-sponsoring a resolution that would see privacy considerations become embedded into the design, operations, and management of information technologies—or at least that is the wish.

A couple of our other files are of great interest to many Canadians: Google Wi-Fi and Facebook. Just this morning, we released our preliminary findings in an investigation of Google's collection of Wi-Fi data by a camera car shooting images for the company's Street View mapping application. We have learned that while collecting Wi-Fi signals, Google had also captured personal information, some of it highly sensitive. The collection appears to have been careless and in violation of PIPEDA. We are making several recommendations that would bring Google into compliance with Canadian law and help safeguard the privacy of Canadians.

But Google isn't the only major technology giant we have had concerns about during the past year. In September, we were able to wind up an investigation of Facebook that was heavily publicized last year. In 2009, Facebook agreed to make certain changes to its site, which took a year to fully and satisfactorily implement. This concluded lengthy and intensive discussions between my office and Facebook, which eventually led the social networking company to significantly boost the privacy protections available on its site.

As we look ahead, I'm looking forward to many other initiatives to strengthen the privacy rights of Canadians. You will, of course, be familiar with two pieces of legislation currently before the House that are of particular interest to my office.

Bill C-28, called FIWSA in English, the anti-spam legislation, would give us important powers to control which cases we investigate and permit the sharing of information for the purposes of enforcing Canadian privacy laws. Earlier I mentioned the Global Privacy Enforcement Network, the group of data protection agencies who together are working toward ensuring better compliance. For us to be an effective member, we need the ability to share information with our international counterparts when necessary, and the provisions in this bill will assist in making that possible.

Bill C-29, meanwhile, would amend PIPEDA to, among other things, make breach notification compulsory for private sector organizations. Over the longer term, we welcome the next statutory review of PIPEDA. We will be publishing in the near future a draft report on the comprehensive public consultations that we hosted this spring on such cutting edge topics as tracking people's online activities by companies, and cloud computing. While this report is not our contribution to the PIPEDA review, the consultations raised issues that we will need to focus on for that review, which starts in 2011.

On the public sector side, we continue to advocate for a long overdue modernization of the Privacy Act, which was passed in 1982. Some of you may remember that 1982 was the year that the first affordable home computer, the Commodore 64, hit the market, and we lined up at movie theatres to watch E.T.

We're also working with experts to develop privacy policy guidance documents for decision-makers working in four key areas. The first, focused on national security, should be ready for publication in the near future, with others to follow in the areas of information technology, genetic technology, and identity integrity.

● (1545)

I hope, Mr. Chair, that I have been able to give you an overall sense of our activities over the past year. I would be happy to respond to your questions.

The Chair: Thank you very much, Ms. Stoddart.

We're now going to go to the first round.

You have seven minutes, Ms. Bennett.

Hon. Carolyn Bennett (St. Paul's, Lib.): Thank you very much.

Commissioner, I think your report on the Veterans Affairs department was certainly one of the most alarming reports that Canadians have seen. I feel that in your commentary on it, you feel that this may not be just in this one department, that it may indeed be the stock in trade of diminishing the reputation of people who criticize this government.

In fact, last week I heard from an injured worker in British Columbia who, because of his workers' compensation status, was being denied mental health access to regular care in British Columbia. It was a very straightforward letter of complaint about this practice and against the Canada Health Act. He was called back from the health minister's office, the Health Canada office, and the person seemed to have every detail of his situation in terms of his relationship with the Workers' Compensation Board of British Columbia.

I will write to you under separate cover for this, but it did make me feel again that it seems that if anybody complains, this government feels it's perfectly okay to open their files and discredit them.

What are you going to do to find out whether these two well-publicized ones in Veterans Affairs are just the tip of the iceberg?

Ms. Jennifer Stoddart: First of all, thank you for the question, honourable member.

I had said very generally that this may be happening in a wider area than Veterans Affairs. It is, of course, a concern of mine, because we reported, for example, that a couple of years ago—this took place a couple of years ago—Canada Revenue Agency civil servants were looking into the tax files of well-known sports authorities, so this is not unknown. I don't have any indication, either personally or institutionally, that this is a widespread practice, but rather that it is an unusual practice.

What are we going to do? First of all, we are going to do our audit of Veterans Affairs and probably report, depending on the timing, directly to Parliament. Second, I'd be very interested if you wrote me outside this discussion today, and we would look into the details of what you relate in your letter.

Hon. Carolyn Bennett: In terms of the need for reform of the Privacy Act, in your commentary and in your final comments here and at international conferences where you have presented, did you have an outline of what would be required in a revision of an act in order for you to be able to do your job properly?

Ms. Jennifer Stoddart: Yes, we did. We made some 14 recommendations to this committee several years ago. This committee looked at the matter in quite some detail, received quite a few witnesses—perhaps 15 witnesses—and came out with a report. The committee supported, as I remember, two-thirds of the recommendations that I made.

However, the Minister of Justice replied that he was not proceeding with reforms to the Privacy Act at that time and encouraged us to look for administrative approaches to privacy problems with the government, so this is what we're doing in lieu of reform of the Privacy Act.

Hon. Carolyn Bennett: Could you give us some international examples? Since the advent of the Internet, of searchable data—since the advent of the Commodore 64, when this act was written—what have other countries done?

● (1550)

Ms. Jennifer Stoddart: Well, most countries either have much newer legislation for the private sector or are contemplating major reforms to it.

I take countries whose legislative models often look like ours. The law in Great Britain, for example, dates from perhaps 2003 and is much more suitable, I think, for contemporary issues. The Australian Law Reform Commission has suggested major revisions to the Australian law, some of which I believe are in effect, but I could't give you any details right now. The European Union is looking at reworking its 1995 directive, which basically governs the privacy parameters for all of the European Union. Within that club, to have a law that dates from 1983 means that we have to be very creative in trying to modernize it.

Fortunately, our other law, PIPEDA, dates from 2000 and has a five-year review, so it's a little easier to work with in terms of modern challenges.

Hon. Carolyn Bennett: In your testimony at the industry committee, you said that you'd not been consulted at all in the decision to scrap the mandatory long-form census. You also said that you'd had very few complaints over the last decade on the so-called intrusion or language. Have you had more complaints since this ongoing mantra of "intrusive and coercive"?

Ms. Jennifer Stoddart: To the best of my knowledge, we haven't received a complaint since June on this topic. I believe we have received some inquiries. I'd have to check that, but we don't have any new—

Hon. Carolyn Bennett: Would it be normal that you would be consulted on a government initiative that was supposedly about privacy and privacy complaints?

Ms. Jennifer Stoddart: Only in the context of a privacy impact assessment. We're not consulted regularly.

Hon. Carolyn Bennett: Are you comfortable that Statistics Canada data is totally anonymous and that it cannot be tracked to the individual?

Ms. Jennifer Stoddart: I am confident now because the rules.... In fact, this was a case that we appeared in at Federal Court. It is now possible, with so much public information out there, that in access to information requests.... This was a case involving drug trials and information gathered by Health Canada. We appeared in order to agree with the Information Commissioner that some fields had to be blocked out; otherwise, the identity of one of the participants in the drug trial could be identified.

Of course, when the Information Commissioner gets such a request, it's referred back to Statistics Canada, and they weigh in. They're very cognizant of the increasing challenges of data-matching with all the information that's out there now.

The Chair: Thank you very much, Ms. Bennett.

[*Translation*]

Ms. Freeman, you have seven minutes.

Mrs. Carole Freeman: Good day, Ms. Stoddart. I am very pleased to see you back here again. You are always welcome at our committee.

Ms. Stoddart, first, I want to congratulate you on the exceptional job that you have accomplished during your time as commissioner. You have been commissioner since 2003, and you have a seven-year term. Unless I'm mistaken, your mandate is set to end in December 2010.

Ms. Jennifer Stoddart: It is November 30, I believe.

Mrs. Carole Freeman: It will be November 30 in one month and a few days.

Ms. Jennifer Stoddart: That is correct.

Mrs. Carole Freeman: Is there a chance that your term will be renewed?

Ms. Jennifer Stoddart: Yes, that is possible under the legislation.

Mrs. Carole Freeman: Would you like that?

Ms. Jennifer Stoddart: I said that I would be agreeable provided it was for a short period of time.

Mrs. Carole Freeman: You do not want another seven-year term?

Ms. Jennifer Stoddart: No, seven years is too long.

As some members of the committee will no doubt remember, when I came to the Office of the Privacy Commissioner of Canada, there were major administrative problems. It took approximately three years to establish our reputation, have a budget and prove that we were a responsible agency. During that time, I was not able to tackle issues relating to privacy protection policy.

● (1555)

Mrs. Carole Freeman: By analogy, you would like a three-year extension. We would like that very much because you have really done admirable work, particularly in recent months on two specific files: the one involving Google's Street View, and Facebook.

I think that you made recommendations on Street View, which had captured personal information using WiFi technology.

I see that your recommendations are of two kinds. First, you mention being able to delete information. You had given them a deadline of February 2011 to resolve the situation and delete data that they had collected. If they were unable to delete that information, it had to be kept more securely, with restricted access. Could you explain to me the second part of your recommendations? In that case, for example, would they be allowed to conserve data that had been collected illegally?

I want to mention that you have done admirable work with regard to Facebook and I want to congratulate you on your work and your leadership, both internationally and nationally. In all areas, you have really made headway on issues related to Facebook.

As soon as you resolve a problem, be it with regard to Facebook or Google, and people seem to be acting in good faith, a rule seems to exist: that of "not seen, not caught." There is always something else that comes out. Now it's WiFi.

With regard to WiFi, they collected information illegally and you are saying that if they cannot delete it, it must be kept securely, or there must be restricted access to it. Under what circumstances are they unable to quite simply delete it?

Ms. Jennifer Stoddart: That conditional clause was included because there are a number of cases currently before the courts involving Google. In fact, the attorneys general of approximately some 40 American states have filed suit under what is called electronic wiretap legislation. There is also another series of litigation cases. In general, when there is a suit, we retain the elements that may constitute evidence.

Mrs. Carole Freeman: These are elements that may be used as evidence in a suit?

Ms. Jennifer Stoddart: We recognize that we cannot order them to do things that they are unable to do under American legislation, since we are working with the American privacy authorities where possible. So we included this conditional clause that states that if 40 states are suing Google, the latter could keep the data and erase it after conclusion of the suit.

Mrs. Carole Freeman: Today, on the front page of the newspaper *La Presse*, we see that Facebook, for its part, was again acting more or less legally. The *Globe and Mail* also talked about this. There was an article that stated that Facebook was offering games such as FarmVille or other games, particularly poker games were people had to register. Based on that, these different sub-groups have a Facebook owner account ID code and they can track that person in order to exchange data.

What do you intend to do in this regard? Will you investigate it?

Ms. Jennifer Stoddart: We have just concluded an investigation on Facebook, two weeks ago.

Mrs. Carole Freeman: I think that Google and Facebook will keep you busy on a full-time basis.

Ms. Jennifer Stoddart: That is, to some extent, the problem.

Mrs. Carole Freeman: They have become very—

Ms. Jennifer Stoddart: You understand the importance of working with other countries so that we are not alone or relatively alone. My colleague from the Spanish National Commission on Information and Freedom issued a press release yesterday that said he was laying criminal charges against Google WiFi for what had happened in Spain, where the system imposes heavy fines.

With regard to your question about Facebook, we will assess this with our technology experts, because it seems that the problem is not coming from Facebook as such, but from applications.

Mrs. Carole Freeman: However, Facebook authorizes those applications. If I have correctly understood the two articles I read in the anglophone and francophone press, when people signed up for Facebook, there were various security standards that were respected. However, as time goes by, the security measures are less and less stringently applied. Facebook is the one that allows games like FarmVille and others on its site. Some laws will be broken and privacy will no longer be respected.

Ms. Jennifer Stoddart: In fact, following our investigation on Facebook, which was concluded in September, part of the agreement specified that Facebook had to respect, under contract, the obligation of using only the personal information that people allowed to be provided, and of only using the personal information they needed for the purposes of the game. That began this summer.

There is still one thing we don't know. We learned about it like everyone else, yesterday, in the *Wall Street Journal*. There was that report, but there was no date on the *Wall Street Journal* investigation. We don't know whether this happened last year, before we concluded our work on Facebook. In fact, Facebook should be ensuring supervision, contractually requiring application developers to respect standards in keeping with Canadian legislation.

We don't have enough specific information on what is really happening, to whom and when. In fact, if it was six months ago, I would say that it was before Google undertook its internal reorganization.

● (1600)

Mrs. Carole Freeman: Thank you.

[*English*]

The Chair: *Merci, madame*.

Mr. Siksay, you have seven minutes.

Mr. Bill Siksay: Thank you, Chair.

Welcome back, Commissioner Stoddart.

I'm glad to hear you're considering another stint at the job. I want to remind you that time flies when you're having fun, so seven years might not be too long. But anyway, I do appreciate the work that you've done in this position in this first appointment.

I also want to recognize that your colleague, your former assistant commissioner, Ms. Denham, has gone to British Columbia to be the privacy and information commissioner there. I'm pleased for her that she gets to stay on the coast now, while I have to fly back and forth, but we're glad that she's taken up that important position there.

Ms. Jennifer Stoddart: Yes, and we miss her.

Mr. Bill Siksay: I'm sure you do.

Commissioner, I want to go back to the situation at Veterans Affairs. I know that all of us are outraged and horrified by what we've learned has been happening there recently and have some frustration, as I know you do, about that situation.

I understand that your original report was a specific investigation into a complaint made by a particular individual. Now you say you're doing an audit of the practices with regard to privacy in Veterans Affairs. Is there some kind of hierarchy of your investigations? Is it an investigation and then an audit? Is there something beyond an audit that you can do? Do you have various descriptors of the kinds of tools you would use to get to the bottom of something?

Ms. Jennifer Stoddart: We have investigations under the act, and they can be broadened into systemic investigations. This tends to be inquiries into a particular set of facts around a particular individual or a series of individuals, looking maybe at patterns and practices, but always related to a specific event.

An audit is I think what we usually understand by its name. It's a general sampling, according to the best scientific principles of representivity, into the practices and the observances of personal information protection in an organization.

We do both investigations, mostly because people complain to us about something. Sometimes we initiate our own investigations, like the Google Wi-Fi one.

What I've announced is that I thought the best tool for Veterans Affairs, given what we were learning, was to do an audit. So that would be a department-wide audit, but only on personal information protection measures.

Mr. Bill Siksay: You've said publicly that you're concerned that this may be happening elsewhere, but you've said again today that you haven't seen any evidence of that. Could a systemic investigation be broad? Could it be across the government, across multiple departments, across the whole government? Do you see that kind of investigation? Or are your systemic investigations more compact than that? What would it take for you to move to a broader consideration of what's happening across government?

● (1605)

Ms. Jennifer Stoddart: It would be a major, major, major operation; I would need quite a few mandates, I think, to accompany that. Our audits usually take a year, although I hope this one could be done faster, and that's in a relatively small department. It's a very big operation.

Mr. Bill Siksay: Do you have the resources to do the kind of audit that you've undertaken now?

Ms. Jennifer Stoddart: Now, in Veterans Affairs, yes, I believe we do.

Mr. Bill Siksay: I want to go the Google report that you released today. I have to say that as a member of this committee I'm concerned, given our initial investigation into Google Street View.

I don't think any of us had any sense that this was anything broader than a street photographing imaging operation that would put up images of what your street looked like and made them accessible through Google Street View. In any of its public discussions of Google Street View, have you seen any indication that Google was collecting other data or was doing anything other than taking photographs and putting them in this particular application on the Internet?

Ms. Jennifer Stoddart: No. Nobody that I heard of in the international data protection or IT community was talking about what happened. What was happening was unbeknownst to all of us until this spring. One of the länders'—they're like the German provinces—data protection supervisors, who have jurisdiction over a lot of the private sector in Germany, started a discussion with Google that quickly became public because they suspected that Google was scooping up personal information.

As I remember the newspaper reports, Google initially denied it, in retrospect because they did not know themselves that they were scooping up personal information. That's how they store...and that's just in April-May of this year.

Mr. Bill Siksay: Is it your understanding—I'm a techno-peasant, so I'm struggling here—that the process they used to gather the street images, the photographic images, somehow required the use of Wi-Fi networks that would put them in contact with this personal information that they had also gathered? Are the two somehow...or is it required, somehow, that it was part of the operation to do an appropriate street imaging and mapping operation?

Ms. Jennifer Stoddart: I'm not a huge personal specialist in this, but I understood that the initial operation was to do a street mapping. Then they were interested in picking up Wi-Fi transmission points for the development of other services, geo-location services. But they didn't understand—because of internal, I'd say, organizational problems—that in doing that they also got the personal information that was unencrypted and not password-protected.

Mr. Bill Siksay: Was Google public about their plan to pick up Wi-Fi transmission points as part of this process? Do you have any indication anywhere that they were public about that part of the process?

Ms. Jennifer Stoddart: I know that at the office.... In fact, Assistant Commissioner Elizabeth Denham, who was responsible for this area, said they had a plan to go on and use geo-location data, which is another field to be exploited by those who are in that business, but nobody had an idea that it involved collecting unprotected information as well.

Mr. Bill Siksay: Okay.

Now, in the report you released today, I notice that at one point you say that your officials undertook a site visit to their operation in Mountain View, California, I believe, back in July. There's a sentence here I wanted to ask you about. It says, “Although our technicians reviewed the payload data, no Google representatives were available in Mountain View to answer our questions.” I think it goes on to say that they did respond by letter to general questions you sent.

Did you get cooperation from Google in terms of your investigation? Or is this an indication that Google wasn't cooperative or wasn't helpful to the work when you were trying to investigate this situation?

● (1610)

The Chair: Mr. Siksay, your time is up.

I would ask the witness to answer, please.

Ms. Jennifer Stoddart: Okay. I'll say that overall they were cooperative, but that maybe there were a few sticky points.

Mr. Bill Siksay: Thank you.

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

Mr. Poilievre, seven minutes.

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

Congratulations on your reappointment and thank you very much for being with us today.

Our government shares your profound concerns with the unauthorized sharing of information by public servants at the Department of Veterans Affairs, and we're very thankful for the work that you've done to investigate it. As a government, we are committed to implementing the recommendations you have summarized here.

Can you tell me what your next steps are on this particular file?

Ms. Jennifer Stoddart: We're doing what's called “scoping the audit”, which involves basically setting up a work plan. This may take a couple of months—Veterans Affairs has offices not only in Prince Edward Island, but also here in Ottawa and across the country—for deciding how we are going to do the work, whether we'll have to contract it out, whether it will be in-house staff that will do it, just how big the sample size will be, and so on. I'd say there's a good few months of planning.

Mr. Pierre Poilievre: When that planning is complete, to what end will you be acting?

Ms. Jennifer Stoddart: We'll be acting to see how this situation that was uncovered in our investigation—and that we and other people read about in media reports of other veterans who dealt with the department—actually came to be. Were there any policies or were they just not followed? How widespread were the problems and what is being done to fix them? What further steps should the department take to make sure that this can't happen again?

Mr. Pierre Poilievre: It seems that the problem goes back to somewhere between 2004 and 2006. We've heard public reports of ministers in the previous government who received the same briefings that have been reported more recently.

What is your sense, given the preliminary work that you've done, of how long-standing this problem has been?

Ms. Jennifer Stoddart: I don't have an idea on that, because we simply look at the very particular circumstances around one person. We didn't go back and sample to see if this was an old practice or a relatively new one. I think perhaps our audit will give us a better idea of that.

Mr. Pierre Poilievre: All right. Thank you once again for the good work you are doing on that file.

On the subject of Google, Wi-Fi, and Facebook, you mentioned that you released your preliminary findings in an investigation of Google's collection of Wi-Fi data by camera cars shooting images for the company's Street View mapping application. You indicate that while collecting these signals, Google has captured personal information of a highly sensitive nature.

Can you be more specific about that? I understand that it might be in your report, but for those who haven't read it, what can you tell us about those signals?

Ms. Jennifer Stoddart: Well, basically these are Wi-Fi signals by which, increasingly, telecommunications or the Internet are passing. A previous member asked what Google knew about it and what we knew about it. I think what is surprising about this file is that this is not something that was done intentionally. This is something that was done without Google itself being aware of the fact that they were scooping up the personal information. A program to take this up was written into the code unbeknownst to those in charge of the Street View photographing program.

This then scooped up data only—before everybody gets too worried—if your Wi-Fi transmission was unencrypted and not password-protected. I think there's a story here for individual Canadians about making sure that they use the strongest privacy protection possible.

Google had been totally unaware that it was getting all this information, but this is not the first time Google has been deficient in adhering to privacy standards, either in Canada or in the European Union, or in other countries that have similar standards.

I think it's a tale of what can happen to your personal information through big technology companies that don't take privacy as seriously as they should.

● (1615)

Mr. Pierre Poilievre: Do you acknowledge that Google has taken some important steps? The reason I raise that is that I was originally called in this committee to investigate Street View, because it was a brand-new application with which there had been no experience anywhere in the world. This was a revolutionary product.

My experience with it since that time has been that the company seems to have taken some very responsible actions to protect the privacy of citizens. I had one constituent who was in a very awkward position when the Street View vehicle drove by; he reported that to me. I have since had a chance to go to his home on Google Street View and confirm in fact that the technology did work, and his windows were obscured, and therefore it would appear that no offence either was endured by him or committed by Google.

So my sense is that there has been a lot of effort taken. Can you tell me specifically what the deficiencies are?

Ms. Jennifer Stoddart: Certainly since early 2007 when Google first started photographing streets outside the United States, they have made great efforts to comply. You talked about the blurring technology for faces, your license plate, and so on. You can have your house taken down or have part of it blurred. That's fine for the Street View photo-imaging product.

But the thing that concerns me is that then we had the Google Buzz fiasco, in which people's identities were revealed one to another without their consent in an attempt to create a kind of social networking within your Gmail correspondence. Your Gmail correspondent could have been, one, your mother, two, your doctor, or three, somebody you had an intimate relationship with. All of a sudden, these people who perhaps didn't even know that the others existed in your life found themselves in an instant social network. That was something that caused us concern. It was almost instantly withdrawn because there was a huge outcry.

Then there was this third thing, which is that, unbeknownst to Google, it was collecting personal information. So it's not that once something is brought to Google's attention they don't clean it up; the question is, why aren't they starting with privacy principles at the beginning? And why are Canadian taxpayers or Spanish taxpayers and so on spending a lot of time and effort when these companies should get it right from the beginning before they launch their products?

The Chair: Thank you, Mr. Poilievre.

Now we'll go to the second round of five minutes.

Mr. Easter.

Hon. Wayne Easter (Malpeque, Lib.): Thank you, Mr. Chair.

I was sure when I was looking at Google Sreet View one night that I saw the Parliamentary Secretary to the Prime Minister standing on the sidewalk and waving.

I'm sure it was you, Pierre. It looked like you—

● (1620)

Mr. Pierre Poilievre: Whoever it was, he must have been a handsome guy.

Voices: Oh, oh!

Hon. Wayne Easter: Anyway, I do have a notice of motion, Mr. Chair, that I want to find time to do a little later.

Coming back to the Veterans Affairs issue, in listening to the parliamentary secretary, there seems to be a move by the government to try to lay the blame for what happened—and it has become public here—on the public servants. So I need to ask you how long it will be before your investigation can really be up and running? When will it end? Will your investigation go right up to and include the ministers' offices, both past and current? If this happened in 2004, it shouldn't have happened. Will that investigation go right up to the ministers, including the ministers' offices?

Ms. Jennifer Stoddart: Honourable member, as I've said, we're planning the audit right now. We're looking at what the scope of it should be. But given the allegations we have heard and what we have found in our own investigation, I think we have to look at all levels of the department to know where personal information is being appropriately sent and not appropriately sent. As I mentioned to another honourable member, we should try to see if this is a traditional practice or a new practice, if we can.

Hon. Wayne Easter: By “all levels of the department”, do you mean the deputy minister's office and the minister's office?

Ms. Jennifer Stoddart: I think it would include at least the deputy minister's office. As you know, there may be some legal issues about ministers being bound by the Privacy Act and Access to Information Act, but that is before the Supreme Court of Canada. Perhaps we'll get guidance at that point.

Hon. Wayne Easter: This government seems to have a penchant for secrecy and a desire to attack anybody who challenges them. We've seen that with independent officers of Parliament, right from Linda Keen on down. We certainly believe that any such investigation should go right to the minister's desk and not stop at the deputy minister. We'll put that on the record.

The second area of questions is related to a *Globe and Mail* story on August 20 about voters lists being made available to others. It was reported that a Brian Patterson made some comments about providing voters lists beyond where they really should be provided now. Brian Patterson—here's just a little bit of background—chaired Tony Clement's federal and provincial leadership campaigns and was the manager for election day for Mr. Clement when he was minister, so he's well connected.

He was asked by a municipal candidate about how to obtain federal voters lists, which the Conservatives manage with a program called CIMS, or constituency information management system. He said:

> But if someone gives you a copy of CIMS in your local campaign, we can't stop you from calling up your local guys that you work [with] on the executives of [riding associations] if you can get it off them. You know, “Hear no evil, see no evil, speak no evil”. “...you never heard me say this—and I'll deny it in a room full of lawyers—that if you can somehow get it, you know, we don't care”.

The Canada Elections Act specifically states that it prohibits sharing voters lists with anyone other than MPs, registered political parties, and federal candidates. Do those kinds of comments from Mr. Patterson concern you—that he may have found a way of...? You know, the lists should just get out there, and they're given to others—other than who they should be.

Ms. Jennifer Stoddart: This is the first time I've heard...or if indeed it was picked up and our press clippings noticed this particular article. I can't really comment on it because this is honestly the first time I've heard about it. We comment on things where we have some personal institutional knowledge of the facts of the case.

I will remind the honourable member of our concern, though, with the potential sharing of the voters lists. A couple of years ago, I believe it was, we did an audit of Elections Canada and were concerned about some of the security issues around the multiplication of voters lists and the distribution of the lists.

As I didn't see this article, I haven't thought about this for a while, but as I remember, there was not a system to get them back at the end of elections, so some could go astray. There were things like that, but I'm not aware of the facts of this article.

● (1625)

Hon. Wayne Easter: We'll provide you with a copy.

The Chair: Okay. That's it.

Go ahead, Mrs. Davidson. You have five minutes.

Mrs. Patricia Davidson: Thanks very much.

Thanks very much for appearing before us again this afternoon. It's nice to see you again. I want to add my congratulations to the other voices around the table for the great work that you've been doing. We appreciate what you've been doing.

Certainly, as my colleague said, we look forward to your audit with Veterans Affairs. Certainly, an inappropriate action has occurred, and we all look forward to getting to the bottom of this issue. We'll all be watching the timeframe of that investigation.

What I really wanted to direct my comments to were the Facebook and Google issues. You certainly are well aware that we have done the Google study here—we've started it, but have not completed it—and are looking forward to hearing from Google again, hopefully in the near future. I must admit that I have not read the report you released today; I haven't seen that report yet, but I will be looking for it in the very near future with anticipation.

I realize that you've been addressing a lot of issues with both Facebook and Google. Can you give us any more of an update about this, on what's been resolved, what's still outstanding, and what might be happening as you continue to work with them?

Can you also talk a little bit about the comment you made in your opening remarks in which you said that later this month you would be at an international conference "co-sponsoring a resolution that would see privacy considerations become embedded into the design, operation, and management of information technologies"? Will this impact Facebook and Google? Is this going to be in conjunction with EU countries? Who will be impacted?

Ms. Jennifer Stoddart: I'll start with the last part of your question, if I may. Every year there is an annual meeting sponsored by privacy commissioners, mostly from the European Union—they have that European-defined level of privacy, which Canada has exceeded—as well as Australia, New Zealand, Hong Kong, and, more recently, some of the Latin American countries. Mexico, I believe, has just adopted legislation; it hasn't been approved as adequate. Uruguay's was. This is a growing movement of countries that have come up to the more stringent privacy standards of the European Union.

Every year at that conference, resolutions are brought forward. They're only resolutions. We try to use them as a way to put forth important ideas and to get public attention focused on the issue of privacy. This year, my colleague Dr. Ann Cavoukian, the commissioner for privacy and information in Ontario, is co-sponsoring this resolution with the host, the Israeli data protection commissioner. I'm very happy to be one of the sponsors.

This speaks to the whole issue of privacy by design. As I was saying in response to a previous question, our problem is not with the product once it's fixed; it's why the privacy wasn't built in at the beginning.

It's very interesting that this concept, which Commissioner Cavoukian has been instrumental in pushing as long as I've known her, I think, has international take-up now. I believe the European Union is considering this issue of privacy by design to be incorporated in their new directive. I guess that's an example of how we try to work together to have some leverage with these enormously powerful international companies.

In terms of ongoing relations, both with Google and with Facebook, I'd say they're positive. Google has very able representation here in Ottawa, and Facebook has great Canadian representation too. The issue is that we're always following after the fact, and it's how to get that message across to them in a way where they really pay attention. Once they're found out and we say, sorry, but this is Canadians' personal information and this is how you have to do it, that's fine, but that process is very arduous for our employees. You can imagine the number of engineers and inventors they have at Google and Facebook, and we have to try to keep up with what they're doing, so—

● (1630)

Mrs. Patricia Davidson: What happens when you do find that there has been an issue? Is there any way of measuring the impact? How are individuals made aware that there could be sensitive information out there? What's the process?

Ms. Jennifer Stoddart: The process in dealing with these two companies, particularly given the take-up on their products, has been to make our reports public, to issue press communiqués, and to try to do public education about this.

I do have that option to make reports public when it's in the public interest. That's a way of cautioning people as soon as we can, by saying: "Be very careful when you're on Facebook", or "If you want to have your house removed from Google Street View, here's what you do". Occasionally people will say, "Well, I tried to get in touch with Google, but I couldn't get my house erased, so can you help us?" In fact, there's some kind of mix-up, and yes, Google will blur—not erase but blur—their car licence numbers and things like that.

Mrs. Patricia Davidson: Thank you.

[*Translation*]

The Chair: Ms. Thi Lac, you have five minutes.

Mrs. Ève-Mary Thaï Thi Lac (Saint-Hyacinthe—Bagot, BQ): Good day, Commissioner. I have a number of questions to ask you.

First, I want to continue along the same lines as my colleagues who asked you about Google Street View and Facebook. I want to know, given the current context of globalization, what legal means can be used to apply Canadian laws to international companies or multinationals.

Ms. Jennifer Stoddart: In our case, the legal means are the Personal Information Protection and Electronic Documents Act. In fact, I do not believe that the Canadian legislation is a disincentive within the private sector, and it might perhaps be appropriate to consider the issue in coming years, if not immediately. As soon as we see that companies are breaking Canadian legislation, we ask them to change their practices. In some cases, they do so, but there are no fines as is the case, for example, in America, England, France and Spain.

At the most, we could say that there are not many incentives for these companies to incorporate privacy protection within their projects from the start. They know that if they are caught breaking the law, that same law allows them the possibility of remedying that before I can take them before the Federal Court of Canada, and then I have to start all over again.

I think that this issue will be raised a lot over the coming year, during the PIPEDA review.

Mrs. Ève-Mary Thaï Thi Lac: You are saying that, at present, the legislation does not include fines. Do you believe that fines should also be set out in the act so as to give it more teeth?

Ms. Jennifer Stoddart: I talked about an international trend. I also spoke about two professors, including France Houle at the Université de Montréal, who did some work for us to determine whether the legislation passed in 2000 is now able to target modern personal information protection concerns. That report has just been submitted to us; I talked about it in my presentations. One of the recommendations is discussing the possibility of having a slightly more coercive regime.

Mrs. Ève-Mary Thaï Thi Lac: I would now like to ask you a question about Blackberrys. Most public servants, MPs and ministers have a Blackberry. When a device is lost or stolen, we call the service provider who tells us that our information will be purged. There is a certain level of security. When the wrong code is entered, after three tries, we are asked to type Blackberry to open the device. The security level is perhaps not up to par when confidential data are being stored.

One of my colleagues recently lost her device. She was told that the data had been purged but she found it, and she was able to restore the data inside. Is it not worrying to know that there is no more security than that with regard to the storing of all the information on such devices?

● (1635)

Ms. Jennifer Stoddart: Your question concerns a number of issues. I do not know whether the Blackberry belonging to your colleague was provided by the government, so if it met government standards. In principle, it should be encrypted. From what I have understood, government Blackberrys are encrypted—the ones at my office are. Perhaps it would be a good idea to protect them with a very good password.

This brings me to one of the audits that we conducted, which suggests that the PIN to PIN function is not used. When the PIN to PIN function is used, it seems, according to my experts, that the department or Parliament server is not being used. So, the signal can be intercepted by quite basic equipment.

Finding one's personal information on a Blackberry is not necessarily bad, to the extent that no one had access to it because it is protected by a password.

Mrs. Ève-Mary Thaï Thi Lac: In your report, you also wrote that government computers are often given to organizations. In news reports, it was mentioned that some data had been erased, but that it was able to be recovered by the organizations receiving those computers.

Following your investigation, what changes will be made to ensure that such data will not be recoverable once they have been erased?

Ms. Jennifer Stoddart: Thank you for your question. The agencies in question noted their inability to erase the information at the workshop, since the workshop was not really set up to erase personal information. We will do a follow up in two years' time.

The Chair: Thank you, Ms. Thi Lac.

[*English*]

Mr. Calandra, you have five minutes.

Mr. Paul Calandra (Oak Ridges—Markham, CPC): Thank you, Mr. Chair.

Thank you, Commissioner.

It's interesting to see.... Brian Patterson, I have to admit, is a constituent of mine, and to be honest with you, I didn't even know he could turn on a computer, let alone access a database, which he certainly has no access to in my office. But I suppose that in the confines of parliamentary privilege and how the Liberals have comported themselves on a number of issues, throwing sleaze around is something that happens from time to time at a committee like this.

I noticed that in your report you mentioned—I'll quote you—with respect to the Olympics that you “came away convinced that the Vancouver Olympic Games provided a valuable lesson in balancing security and privacy rights at mega-events—lessons that could be refined and applied again at future national or international gatherings on Canadian soil”.

Of course, I think we are all proud of the Olympics and the type of year we've had with respect to holding international events. I'm wondering if you could say, in comparison to other jurisdictions, whether Canada has become a leader in balancing privacy and security at the same time.

Ms. Jennifer Stoddart: I think Canada is well respected for its balancing of these two rights. We have a very thorough process. It's not in all countries, for example, that things like the airport scanner, to take that particular one, are referred to the Office of the Privacy Commissioner for a privacy evaluation. I think that has attracted a certain amount of attention. I know that on the level of scholarship, there are a couple of international scholars who are interested in working with us on how to balance the principles of privacy protection with national security imperatives.

● (1640)

Mr. Paul Calandra: I also want to just follow up on something that Madame Thi Lac had mentioned with respect to computers and data.

Are there actually rules with respect to how these computers—or any data, for that matter—are supposed to be cleaned? In your investigation, did you find that departments aren't actually following the rules? Is that one of the reasons...? Should we be tightening up? Should we be perhaps considering tighter rules or re-educating the public service with respect to how we do this?

Ms. Jennifer Stoddart: Well, yes, one wonders. The rules have been there for a long time. In fact, 10 years ago, the commissioner who preceded me, Bruce Phillips, did an investigation of this kind and found that there were an enormous number of computers that were not being wiped clean.

My take on this is that at the end of the 1990s we were all just starting to work with computers and maybe we didn't realize that everything is indelible unless it's specially wiped and so on. But we thought, for interest, that we would follow up 10 years later to find out what was happening.

In our sample, 40% of the computers had not been completely wiped. There was still personal information on them—in fact, national security information—in spite of the clear directive that has been around for more than 10 years, and in spite of, I would say, increasing popular personal individual knowledge of what happens on the computers we all work with, whether they're little BlackBerrys or much more powerful ones.

This was a bit of a surprise to us. It's not that the rules aren't there, but I guess busy people forget that, or the job's half done. That's another audit we'll be following up on in two years.

Mr. Paul Calandra: I come from the insurance industry. I was an insurance broker. I remember that the introduction of PIPEDA was something that was very confusing for us in the early years. There is still a lot of confusion, I think, with respect to it, certainly in the industry that I was in. You found some organizations that were very aggressive with respect to how they treated personal information and to signing off on the information that was provided.

Is there still some room for education? I know the answer is going to be yes: there has to be some room for educating private business with respect to the collection of information and how important it is, and perhaps clarifying and helping them understand the importance that our government places on the privacy of people. Do you have any suggestions on how we can actually educate a bit better in the private sector?

Ms. Jennifer Stoddart: Yes. In fact, educating small and medium-sized businesses would be an objective for the next three years—if I continue on for three years—because we realize, partly because of the work of these two university professors, that big business, like the big insurance companies, the big banks, and so on, are following the rules pretty well. They're pretty sophisticated. We rarely have serious complaints against them now, and if we do, they're quite rapidly settled.

The issue with small and medium-sized businesses is that this is seen as an extra financial burden—and it probably is—for them, as just another thing they have to do. We're working on a program, particularly out of Toronto, where a lot of Canadian business is centred, to take some of the tools that have been developed by big business and, with them, try to adapt them. So these would be tools that small and medium-sized businesses could access free of charge through our office so that they don't have to go out and spend $200 or $300—sorry, $3,000—on a custom-made.... There should be something that is reasonably adapted, that can be scaled down from the bigger business experience.

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

Mr. Bill Siksay, for five minutes. I'm having trouble with that name; I will get it, Mr. Siksay.

Mr. Bill Siksay: You will get it yet, Mr. Chair. It's like “apartment 6A”; it's not “apartment 5B”.

Some hon. members: Oh, oh!

The Chair: It's that “k” in there that's driving me crazy.

Mr. Bill Siksay: I know: the mysteries of the Anglo tongue.

Thank you, Mr. Chair.

Commissioner, I wanted to come back to your investigation report on the situation at Veterans Affairs. You made some specific recommendations to the department, some for immediate steps. I know that wasn't so long ago. Have you heard back from the department on that? Is there any follow-up yet in terms of what's in place?

Ms. Jennifer Stoddart: Not that I'm aware of, no.

Mr. Bill Siksay: In some of your reports, you negotiate. I know that in PIPEDA, you work with the offender—that's not quite the right word—or the entity to come up with recommendations in a process. Is that true with the Privacy Act too? Did you work with Veterans Affairs on developing these recommendations and have they signed off on them by the time you make your report? Or is this a different process?

● (1645)

Ms. Jennifer Stoddart: The recommendations are shown to them. They have a chance to comment on them, to make factual corrections to the report and so on. Whether we negotiate, as you say, or try to arrive at a consensus, depends on the type of issue we have.

Here we have an issue where it seems there were multiple illegitimate accesses to somebody's personal information, so it's not something that you can really negotiate on, going backwards. But forward, I didn't hear that there was any objection by the department or the officials to any of the recommendations that we made going forward, nor indeed to an audit.

Mr. Bill Siksay: The first recommendation was, “Take immediate steps to develop an enhanced privacy policy framework...”. What is “immediate?” When would you think something like that should be in place, given the seriousness of this situation?

Ms. Jennifer Stoddart: For taking “immediate steps”, I would say in the days and weeks that follow. If this is a widespread issue, it's pretty critical.

Mr. Bill Siksay: So we're within that timeframe now in terms of when you released your report.

Ms. Jennifer Stoddart: Exactly.

Mr. Bill Siksay: Commissioner, just in terms of the Google Street View issue, when the committee was doing work on this—and it was some time ago now—we heard from another company, Canpages, that was using a similar process. Do you know if there are similar issues in terms of the collection of other data from other companies that are using a similar process? Have you looked into that?

Ms. Jennifer Stoddart: Yes. That was one of the subjects of our consultations this spring. We are working on that. We're bringing out a position paper.

Google is not the only one dealing with geopositional location technology; some of it could be quite privacy-invasive. What we haven't done is look at the different individual types in terms of even our investigation or not...we're looking at them as examples of deploying a new technology.

Generally, I believe that former Assistant Commissioner Elizabeth Denham did some informal work with Canpages—and I believe there is another company whose name I just forget—in terms of them giving notice in a way that Google never did when they were about to photograph or geomap a certain area.

Mr. Bill Siksay: You're saying there may also be incidents where they've collected personal data because of the kind of process that was involved?

Ms. Jennifer Stoddart: Yes. I don't believe the process itself is illegal in Canada. The issue is taking the personal information without notice or any form of consent. I haven't really thought of this for a while, I must say, but I believe that we worked with Canpages, so they gave the best type of notice they could, given the technology they're working with. I could get back to you on that.

Mr. Bill Siksay: So it may be possible that other companies are collecting Wi-Fi transmission points and that kind of thing from using a similar kind of geomapping cartographic process?

Ms. Jennifer Stoddart: Exactly, and using it eventually to send messages to people on their hand-held devices about all kinds of things. In fact, we used those scenarios in the consultation.

Mr. Bill Siksay: In your annual report, you noted that you thought companies offering this kind of street-imaging application could be doing more in terms of improving notification and blurring technology. Can you say anything more specific about it? Is there something you've asked them to do specifically with regard to those two things?

You've just mentioned improving notification. Can you say something more specific about what kind of notification you would like to see and what problems you've identified with the blurring technology that's in use?

Ms. Jennifer Stoddart: Well, I guess reasonable notification that would get to a wide variety of people whose whatever they had was about to be photographed...maybe not just a newspaper, but maybe some radio advertisements or interviews, things that would get people's attention, so that if they had a problem, they would know how to get in touch with the company.

In terms of blurring technologies, I think we had about a two-year discussion between some of the specialists in my office and Google about the strength of their swirl technique and whether or not it could be unswirled. Do you remember the case of a gentleman who had gone to Thailand and then his swirl was unswirled? That took a while to settle, but it seems to be a fairly strong technology now.

● (1650)

The Chair: Mr. Siksay, your time is up. Thank you very much.

Mr. Easter, you have five minutes.

Hon. Wayne Easter: Thank you, Mr. Chair.

This is a case that came to our office and does relate to privacy issues. The RCMP, for all the right reasons, have implemented a real-time identification program. I don't know if you've had any of these cases. For the RCMP, it's to ensure that they can call upon rapid access to fingerprinting services.

One of the side effects of this is that if you happen to have the same name as someone who has a conviction and have a birthday quite close—which is the case in this case—and you're applying for a job, then you have to submit yourself to fingerprinting to clear your name. Have you had any of those cases or do you have any advice on where we can go on this?

Ms. Jennifer Stoddart: I don't have any details of that, but I know that we are working with the RCMP in terms of a privacy impact assessment. I believe we are encouraging the RCMP to possibly narrow the scope and the application of this program, but I don't really have the details here, so I'd have to get back to you on that.

Hon. Wayne Easter: Okay, if you could, please, because certainly you don't want to have to submit to fingerprinting, but I also understand the bind the employer is in. You apply to the RCMP for a criminal check, it comes back, and I guess they have no way of knowing if the names are not the same. But then you have to submit yourself to fingerprinting. It is a problem.

I have no further questions, Mr. Chair.

The Chair: Thank you, Mr. Easter.

Mr. Poilievre, you have five minutes.

Mr. Pierre Poilievre: I just want to confirm for the public record if you've had any news about your reappointment.

Ms. Jennifer Stoddart: Yes. I've been contacted by the Prime Minister's Office. I believe the Prime Minister has written to the leaders of the opposition parties to ascertain their views on a further reappointment for three years.

Mr. Pierre Poilievre: Can you explain to us why it would be for three years instead of the normal term?

Ms. Jennifer Stoddart: Honestly, 14 years as a privacy commissioner in this fast-changing world would be too long. As I perhaps mentioned, I did spend a lot of time doing very intense administrative work at the beginning of my mandate, so I think I have the energy and interest to go forward for another three years on some of the increasingly interesting and challenging privacy issues.

Mr. Pierre Poilievre: So three would be your preference?

Ms. Jennifer Stoddart: That's right.

Mr. Pierre Poilievre: I don't know if anyone wants to take the remainder of my time.

Mrs. Kelly Block (Saskatoon—Rosetown—Biggar, CPC): I can do that. Thank you very much.

Thank you very much for being here today, Ms. Stoddart.

I echo my colleagues' comments both on the issues that have been raised about Veterans Affairs and on the work you have done in your role as commissioner.

My questions are focused on the report you recently tabled and specifically on sections 4.2 and 4.3. Section 4.3 is on “Complaints Closed”.

Ms. Jennifer Stoddart: Excuse me, honourable member, is this the Privacy Act?

Mrs. Kelly Block: Yes.

One can understand the impact that you and your staff, through focused efforts, have had in the area of complaints closed. As has been mentioned already in congratulating you on your reappointment, you have done tremendous administrative work in this area.

But I'd like to focus on section 4.2. I notice that the number of complaints and investigations are down this year by approximately 12%. Can you share some possible explanations for that?

● (1655)

Ms. Jennifer Stoddart: First of all, we've spent an intense four years trying to get rid of a backlog that started to accumulate in the early years of this decade. Fortunately, we had budgetary support, so we eliminated it at the end of the last fiscal year on which we're reporting it.

Concurrently, we're trying to do something in parallel, which is not to refuse to help Canadians, but to answer their questions and help them with their problems at the outset. Very often we see that when people get the information they desire, they can go off and solve the problems themselves, or we can put their minds at rest without going through a whole investigation. Because the Privacy Act is fairly dated, the investigations take on a formal aspect that is long and not necessarily helpful to the individual person, who usually just wants access to their government file.

So that explains why the complaints are down. From an administrative point of view, I think we should stay with the same budget. This is not a time to be increasing it. So if we spend less time on individual complaints—there's already a model wherein this issue is being dealt with and we can refer somebody to it—that frees up resources for some of the big investigations that are very resource heavy.

Mrs. Kelly Block: Thank you.

The Chair: Thank you very much.

Before we go to the third round, there's one area I'd like to canvass with you, Madam Commissioner, and that is the budget for your office. Of course, Parliament gives final approval, but the original submission is developed by Treasury Board, with considerable input from the panel on the financing and oversight of officers of Parliament. It's relatively new. It's been in existence now for five or six years.

Can you give us your comments? Are you reasonably satisfied with the input of this panel?

Ms. Jennifer Stoddart: Yes, our experiences have been positive. The panel has brought together, in a very innovative and positive way, parliamentarians, Treasury Board officials, and us as the organization that requests the money. We talk to Treasury Board beforehand, so all the budgetary requests we make have the support of Treasury Board. We answer the questions as to why we need this money. In our case, we have the resources we asked for.

The Chair: From your testimony here today, it seems to me that your office is embarking on some relatively major initiatives—the DVA issue, the Google issue, and the Facebook issue, among others. In your opinion, do you presently have sufficient resources to carry out the mandate you've been given by Parliament?

Ms. Jennifer Stoddart: I think so at the present time. I know that we're under economic constraints. One of the things I'd like to do in the future is continue to try to find ways to work more efficiently, perhaps by the use of things such as online complaints and increasingly turning to the Internet as a way of interfacing with Canadians.

What would be helpful as an agent of Parliament, I think—and as you know, for certain things we're in a different world than government ministries—would be some flexibility in the administration of the budget, which we don't have. This is something that we've recently realized is a challenge. It is not necessarily to get a new budget or to overrun our budget, but simply to administer the different budgetary posts as we choose.

The Chair: In your opinion, Ms. Stoddart, in the fulfilling of your office's mandate, are you receiving cooperation from all departments and agencies within the Government of Canada?

Ms. Jennifer Stoddart: Yes, I think cooperation has been very good. I'm not sure that people are really happy to see us coming. I think that if there were a popularity contest, certainly we wouldn't win it.

There has been cooperation. There is respect for the functions of the office and also an understanding by departmental officials that what we do is important, even though they're not always happy to see us and we raise uncomfortable questions.

The Chair: As I have indicated, we've concluded the second round.

We're going to go to the third round now. You will have five minutes each.

We're going to start with Ms. Bennett.

Ms. Bennett, you have five minutes.

● (1700)

Hon. Carolyn Bennett: Somehow it makes it easier for a commissioner if the departments actually have a culture of divulging when there's been a mistake. We've learned from the airline industry that you don't lose your licence for making a mistake; you lose your licence for failing to report a mistake.

I think in the ongoing interest of the privacy of Canadians, departments need to feel comfortable reporting a possible or real breach in the data, such that it turns into a learning culture, where you could tighten this up because the department says, whoops, this happened.

Yet we all know that within departments there's a sort of risk-averse culture. If you've made a mistake or almost made a mistake, there's a sort of gotcha feeling or a reluctance to admit that there was a mistake.

Do you think we're getting there, that departments are feeling more comfortable reporting a possible breach or a real breach rather than waiting until it is caught or comes from a complaint-based system?

Ms. Jennifer Stoddart: Yes, that's a very important question. I think that on some page of this annual report, we report on a growing trend by departments to report privacy problems to us, departments that aren't legally obliged to, including losses and breaches and so on, in the hope of getting some help with this.

Increasingly we're trying to focus on a collaborative, preventive role, because you know, if people are going to be punished, they don't come forward. The issue is how to not keep repeating the same problems, or at least to make sure that they don't happen again in exactly the same way. This is a trend and I'm very happy about that.

Hon. Carolyn Bennett: When asked about resources, you said that you thought you had sufficient resources to do the audit within Veterans Affairs. In terms of the privacy impact assessments, It looks like you've had a 60% jump in submissions. Do you think you have enough resources to do these in a timely fashion?

We congratulate you on getting rid of the backlog, which is the complaints-based system, but do you have the tools to do it proactively with audits and impact assessments? How do you decide which would be the most important ones to do, given the limited resources?

Mr. Chair, in terms of this committee, will we write a report that would allow the commissioner more flexibility in terms of the way she administers her budget? Is it possible for us to do that, Mr. Chair?

The Chair: Definitely: we can write any report we want, and that report would go to government, Ms. Bennett. Perhaps we can ask the commissioner to elaborate on that. There are probably results of some of the problems that this office had before Ms. Stoddart became the commissioner. This particular office has had problems in the past, as we're all aware, and there may be some constraints as a result of previous issues.

Am I right in that, Ms. Stoddart?

Ms. Jennifer Stoddart: No. These are not constraints because of previous issues. That was what was happening in the first three years of my mandate. We got back our full powers and full confidence.

Perhaps, Mr. Chair, I could answer the question of the honourable member: how do we then choose with limited resources? We look at our privacy impact assessments and choose the ones that, after a first initial examination, seem to us to be the ones that put Canadians' personal information most at risk.

Hon. Carolyn Bennett: In some of the legislation that died on the order paper, you had some concerns. Have you been consulted on what was the previous Bill C-46, Bill C-47...? Do you anticipate that your concerns will be dealt with if those bills are tabled again?

Ms. Jennifer Stoddart: They have not been tabled as such, for which I am very happy. We did in fact consult extensively ourselves and then wrote a preliminary letter to the Minister of Public Safety last fall. Some of the content of those bills or the purpose of the bills is now enshrined in, I believe, Bill C-29, and certainly that's an improvement on what we saw last summer.

● (1705)

Hon. Carolyn Bennett: But do you routinely see bills beforehand for a privacy assessment?

Ms. Jennifer Stoddart: No, we don't.

Hon. Carolyn Bennett: So do they table things that could be a problem and then find out afterwards?

Ms. Jennifer Stoddart: Yes. But in some cases, when it is a matter that comes under our particular jurisdiction, often there is informal consultation between ourselves and department officials. But we don't see the legislation per se before it's tabled.

The Chair: Thank you very much, Ms. Bennett.

Mr. Albrecht, five minutes.

Mr. Harold Albrecht (Kitchener—Conestoga, CPC): Thank you, Mr. Chair.

Thank you, Commissioner, for being here today.

I'm a recent appointee to this committee, so I don't have the long institutional memory that many of my colleagues here have. I just want to follow up a bit on the training or the provisions for members of the community to know what their obligations are.

On page 11 of your report, relating to the mortgage brokers, you indicate:

> The Mortgage Brokers, Lenders and Administrators Act, 2006 requires mortgage brokers and agents to undertake specific training concerning the provision of mortgages. While we found that brokers and agents had undertaken this mortgage training, no agents from the mortgage broker companies that we audited had been provided with formal and ongoing training under company-specific privacy practices, or their responsibilities under PIPEDA.

I think it's quite possible and probable that many of the employees or individual brokers or agents had actually acted in ignorance and may not have been aware that there actually had been a privacy breach.

Now, I'm sure that most departments have strict safeguards to ensure that personal information is secure and that their employees are well trained in their efforts to protect their documents. I understand you said a few minutes ago that in your next three years you're going to focus more on the training aspect, especially related to private agencies, but my question is, what kind of current training does your department do beyond what private companies like this, or even individual departments in government, would provide to their own employees?

The second part of that question is this: if you could guess, what percentage of the breaches that occur would you think are simply human error, or ignorance, as opposed to wilful ignoring of the guidelines?

Ms. Jennifer Stoddart: First of all, what do we do for businesses already? We have extensive material on our website. Increasingly, we use our website, because it can be accessed by Canadians across Canada. We have just updated our tool kit for small business in consultation with the small business communities. As I've said, we hope to continue that in the future, using some of the material borrowed from the experiences of larger companies that can be adapted.

We consult with various representatives of the small business community regularly, and if they say they need *x* number of information sheets for their kits at a conference, we are happy to provide them with those. We have some that are done particularly for businesses.

This might seem a little frivolous, but we have worked on a series of cartoons. I think we have about 20 different cartoons now that are very useful for public education. It's hard to get the attention of the business person who's worrying about their balance sheet at the end of the month, so maybe somebody in a presentation in a local community can use one of our cartoons, and it might get their attention. Then maybe they'll go on and listen to the short message and explore this by themselves.

Those are some of the things we want to do.

We're also cooperating with the provincial commissioners across the country to provide them with templates for personal information in areas where either we have jurisdiction or sometimes there's a kind of overlapping jurisdiction. Or they can serve as the distribution point, in a collegial fashion, for materials and messages about small business if we have a jurisdiction in a province, for example, like Saskatchewan. So we do things like that.

Finally, what percentage of data breaches are human error? I would say probably between 40% and 60%. It depends on what sample you look at. It's not all about thieves and hacking into computers and so on. Often it's just employees who make human errors, as we all do, and now the errors are amplified by the technology, so it's in fact more stressing, I think, not to make an error now.

● (1710)

Mr. Harold Albrecht: Do I have any time left, Mr. Chairman?

The Chair: Go ahead, Mr. Albrecht.

Mr. Harold Albrecht: In relation to your international investment of time and energy, would you have a rough idea as to what percentage of your department's resources are invested in developing international policy to address the issues you've mentioned in your statement about the resolution to see privacy considerations becoming embedded in the design?

Would you have a rough idea as to what percentage would be committed to that international component? Because the computer world is a borderless world, as we know.

Ms. Jennifer Stoddart: I guess we've never looked at it that way, but maybe it's 10%. I'm just saying.... I have the director of finance here, but I don't think even he has ever calculated that.

We do it because, once again, we think we can be more effective. If it's Canada alone on this technology, well, you know.... If we have a strategic alliance, we'll have much more effect.

The Chair: Thank you, Mr. Albrecht.

[*Translation*]

Ms. Freeman, you have five minutes.

Mrs. Carole Freeman: Thank you, Mr. Chairman.

I have two questions for you.

My first question deals with national security. On page 54 of your report, you mention other measures related to public security. At the Olympic and Paralympic Games, you played a role alongside the organizers, who asked you to work with them. Can I know what the nature of your role was? As is mentioned in your report, the Olympic Games were the biggest event since the attacks of September 11. I find this interesting and significant. What was your role?

Ms. Jennifer Stoddart: On the one hand, our role was—

Mrs. Carole Freeman: Could you please respond briefly, because I have another question for you.

Ms. Jennifer Stoddart: On the one hand, our role was to work with the police, the RCMP, to make officers aware of issues relating to privacy protection, and, on the other hand, to inform members of the public of their right to privacy.

Mrs. Carole Freeman: What exactly did you do to help the police in terms of privacy protection?

Ms. Jennifer Stoddart: We met with police forces several times.

Mrs. Carole Freeman: What kinds of problems were you expecting?

Ms. Jennifer Stoddart: I will try to give you a brief answer. At that time, there had been allegations that the police was misusing people's personal information at the border with the United States, that activists in Vancouver were under increased surveillance, and that there was a database on the activists, and so on. This was before the games. Nothing happened, but I remember that the atmosphere was fairly tense before the games.

Mrs. Carole Freeman: As a Quebecker, I feel very strongly about what happened at the G8 and G20 summits. Many of my fellow citizens went to the summits and were arrested, and they told me that their personal information had been used. At the G8 and G20 summits, did police forces ask you for help or to work with them as far as personal information was concerned? I really want to understand why people called on you. Were you called in to help the police target activists? Were you asked to work with authorities at the G8 and G20 summits?

Ms. Jennifer Stoddart: No.

Mrs. Carole Freeman: You were not called upon?

Ms. Jennifer Stoddart: As far as I know, nobody called upon us for that. Further, I do not believe that those events fell under federal jurisdiction. As far as I know, the Ontario Provincial Police and the Toronto Police do not fall under federal jurisdiction.

Mrs. Carole Freeman: The RCMP was there, as well.

Ms. Jennifer Stoddart: The RCMP was there, but—

Mrs. Carole Freeman: The RCMP falls under federal jurisdiction. Did it not occur to you to offer your services to the RCMP to help the other police forces use personal information to target the activists?

● (1715)

Ms. Jennifer Stoddart: On the one hand, we had just put the Olympic Games behind us, and so we thought that the lessons from the games had been learned and integrated. On the other hand, I do not believe that we were called upon because, contrary to the games, nobody had expected these events to happen.

Mrs. Carole Freeman: It was a dark moment in the history of democracy and the respect of people's privacy. What happened at the G8 and G20 summits was absolutely horrible.

Here's my second question. I know that in 2009, the world we live in, which is increasingly online and borderless, was the dominant theme of the work carried out by the Office of the Commissioner. In fact, last April, it was very surprising that you established the four following priorities: information technology, national security, the integrity and protection of personal identity, as well as genetic technologies.

Can you tell me what the major challenges and priorities will be for you in the coming year?

Ms. Jennifer Stoddart: We will maintain these four priorities because it will take years for us to study them in depth. Over the coming years, they will remain very significant priorities. Indeed, our objectives will include increasing the efficiency of our office and improving our contacts with the business community, which will happen, for instance, because we will be present in Toronto.

Mrs. Carole Freeman: Thank you, Ms. Stoddart.

The Chair: Thank you, Ms. Freeman.

[*English*]

Mrs. Davidson, five minutes.

Mrs. Patricia Davidson: Thanks, Mr. Chair. I'm going to share my time with Mrs. Block, if I may.

I notice in your opening remarks that you talk about developing policy guideline documents and that you're working on them in four key areas: national security, information technology, genetic technology, and identity integrity.

Can you elaborate a bit more on that? Who are you collaborating with to develop these? What do you expect the advantage will be to have them done? What is the timeline?

Ms. Jennifer Stoddart: We're working right now on the national security document. There's a bit of a debate, in fact, about who it will be useful to. First of all, it's a public document, of course, but the idea is that it is directed to government policy-makers who have to take security considerations into account and also, to the extent possible, protect privacy as well.

That is the one we're working on. We work with a variety of people: scholars, people in government security, and the police community. We have a former foreign affairs minister on the committee, and we have members of the advocacy groups that are very interested in civil liberties, to try to get a complement of different points of view so we have some kind of general guidance on what, from the point of view of the Privacy Commissioner, we consider to be a good balance between these two objectives. That's the one that we've really come the farthest with. It's a similar process in terms of genetic information.

Mrs. Patricia Davidson: Thank you.

I'll refer it now to Ms. Block.

Mrs. Kelly Block: Thank you very much, Mr. Chair.

In a follow-up to my previous question and perhaps to my colleague's question around your public education efforts, I want to turn to your PIPEDA report. In that report, it points out that in 2009 there was a 20% drop in new inquiries, from 6,344 in 2008, to 5,095 in 2009.

I'm wondering if you can tell me why you think that is the case. Is it similar to the drop in complaints when it comes to the Privacy Act? Could I get your comments on that, please?

Ms. Jennifer Stoddart: We think it's something like what happens in the Privacy Act and my previous response, but this time we saw the drop in inquiries accompanied by a rise in the number of people who go to our website. We now have about 2.5 million on our website, and we're trying to continue that, because people can get the information they want. We have a children's website, our youth privacy website, a blog, and so on.

Mrs. Kelly Block: If I could quickly follow up on the comments our chair made when he was asking you about the cooperation between your department and other departments, there's a comment on the Privacy Act, again in section 4.2. It says, “The number of complaints filed against an institution does not necessarily mean the organization is not compliant with the Privacy Act”. Could you elaborate on that a bit?

● (1720)

Ms. Jennifer Stoddart: Yes. Over the years some people have asked why we don't do a report card and rate all the departments and so on. This may be appropriate in some circumstances, but it doesn't seem to be appropriate for what our office does. Some departments, by their very nature, have to hold a lot of Canadians' personal information, so on a representative basis they're going to get a lot of complaints.

The single department that has the most requests year after year—I think probably since the office was opened—is the Correctional Service of Canada, because of course it controls all the personal information of the people in their files. Also, it has a problem with replying within 30 days, so then there's another complaint.

It goes down in that order. The RCMP has a lot of complaints, again because of its function. Ironically, for some places where there may be systemic problems, like Veterans Affairs, there are statistically very few complaints.

The Chair: Ms. Block, your time is up.

We are now going to move to Mr. Siksay. Then Mr. Easter has a motion, and then we will adjourn.

Mr. Siksay, you have five minutes.

Mr. Bill Siksay: Thank you, Chair.

Commissioner, I want to ask you about privacy impact assessment reviews, and one in particular. You mentioned that some places in government appreciate your work, but they're anxious when they see you're coming.

I'm assuming that one of the people you may have been thinking about is the President of the Public Service Commission, who had some concerns about how you reported on the privacy impact assessment review of the political impartiality monitoring approach, which you report was an attempt to collect information on the private activities of public servants. The President of the Public Service Commission said she thought the language was too strong and that you were misleading in terms of the intent of the program, although it seems like the program was scaled back as a result of your intervention.

I wonder if you could comment about that and how that process works, and your concerns about that program.

Ms. Jennifer Stoddart: Well, we tried to report as objectively as possible our concerns with the first draft PIA and the description of this program and what it was set out to do. It was something that we had never seen before as a proposal, and what we understood was that it was a proposal to scan the web for indications of political activity. In talking with the commission, it was agreed to take it back, look at the program, and provide us with a new privacy impact assessment.

I think somewhere there's an acknowledgment that perhaps we have raised some relevant questions, such as, "Why this program?" In order to scan somebody's political activities outside of the government.... Has there been something like a radical increase in the remarked political activities of civil servants that would cause this? What we understood was that it was looking at personal websites, at blogs and so on.

Anyway, we're waiting for the second version of this, and we hope we can continue dialoguing about this and see eye to eye on it.

Mr. Bill Siksay: So you haven't received the second run-through of it yet?

Ms. Jennifer Stoddart: No, we haven't.

● (1725)

Mr. Bill Siksay: I appreciate that you are working on this, because it strikes me as a very serious issue. I do share your concern about it and I appreciate that you've taken it up.

I wanted to ask you about another issue, which is the situation of border crossings. There are a number of issues. There is some report of it in your annual report, but there were also newspaper reports.

One in particular was about a Montreal student who had a laptop searched by the U.S. authorities at the border. One of your colleagues, Anne-Marie Hayden, had responded that "Canadian courts have recognized there is a 'diminished expectation of privacy' at border crossings". I'm just wondering... Is that something you accept: that there should be a reduced expectation of privacy at border crossings for Canadians or for people coming into Canada?

Ms. Jennifer Stoddart: I think I have to accept that for a long time it has been recognized that nations are sovereign and they control the conditions upon which they let citizens of other nations come in. They can set those rules.

What I don't accept is that there are frequent complaints by the public about the manner in which they are treated at the border, so we are working with the Canada Border Services Agency to see if we can sensitize some of the border guards or officials to the impact of some of their words, their gestures, the way they treat Canadians coming back into the country, and how these things make them feel as though their privacy has been invaded and so on.

We can't change that reality, but we could help to encourage a more sensitive treatment of people.

Mr. Bill Siksay: You have developed a resource for people, which I think is called "Checking In", about dealing with security and customs at the border.

Ms. Jennifer Stoddart: Yes, we have.

Mr. Bill Siksay: Has there been significant uptake on that resource? Or is it one that you consider successful? Has there been an evaluation of its success?

Ms. Jennifer Stoddart: I can't answer that question. I could get back to you on it.

Mr. Bill Siksay: It would be interesting to know.

If there's time, I just want to ask one other question about full-body scanning at the airport. Recently in the newspapers and in media reports, you noted that there is a new generation of machines coming on that will "more sharply" define the images that are used. I am wondering if that changes your view of this technology. Have you seen anything about Canada moving towards using that new technology? Where are we at with these full-body scanners at airports?

Ms. Jennifer Stoddart: For the moment, we are using a less intrusive type of scanner, the name of which escapes me. This is not the most intrusive, which may be the backscatter x-ray scanners, some of which have been introduced into the United States and which apparently put the human body into, shall we say, detailed focus as compared to the one currently used in Canada, which my office has tested out. People of both sexes have tested it out. It shows, as I understand it, foreign objects on an outline of the body, so it is much less privacy-intrusive.

In the quote you read, I was asked to say what keeps me "up at night", and I said that if national security issues became so imperative that there was a push to move to these, then yes, that would be a huge privacy challenge.

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

There is just one minor issue that may be dangling. I'm not going to ask for a response, Ms. Stoddart, but you did mention—and it may not be an issue—that there might be some concern with your ability to allocate funds within your department. If there's still an issue, I invite you to write a letter to the committee and we can follow it up. I'm not looking for an answer now.

Mr. Easter, you have a motion.

Hon. Wayne Easter: I'd just like to read a notice of motion into the record, Mr. Chair, so that it could be discussed. The motion reads as follows:

> That the committee requests that Nigel Wright provide it with copies of any agreements with Onex Corporation for him to return from temporary leave to the corporation. The committee also requests that Nigel Wright provide copies of any recusal conditions that he has agreed to abide by as Chief of Staff to the Prime Minister to ensure that he is not in conflict of interest. And that the information be provided to the committee within 5 days.

I so move for notice.

The Chair: That is just for notice, Mr. Easter, and that of course won't be debated today.

That, colleagues, concludes the meeting.

On behalf of everyone on the committee, Ms. Stoddart, I want to thank you. As I stated at the opening of the meeting, the commissioner did come here on very short notice. She had to rearrange her schedule to accommodate us and we're very thankful.

Thank you very much.

Ms. Jennifer Stoddart: *Merci.*

The Chair: The meeting is 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