HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 034 • 1st SESSION • 41st PARLIAMENT

EVIDENCE

Thursday, April 26, 2012

Chair

Mr. Pierre-Luc Dusseault

Standing Committee on Access to Information, Privacy and Ethics

Thursday, April 26, 2012

● (1105)

[*Translation*]

The Chair (Mr. Pierre-Luc Dusseault (Sherbrooke, NDP)): Good morning, everyone.

I want to thank Ms. Stoddart and Ms. Bernier for joining us today.

As you have seen, based on today's agenda, the first hour will be set aside for the two reports. The first is the 2010 annual report on the Personal Information Protection and Electronic Documents Act, and the second is the Privacy Commissioner of Canada's 2010-2011 annual report.

Mr. Alexandre Boulerice (Rosemont—La Petite-Patrie, NDP): Mr. Chair, I would like to take a moment to announce to the committee and the clerk that today I will put forward a motion I would like us to debate next Tuesday. The motion asks that Claude Benoît, President and CEO of the Old Port of Montreal Corporation, appear in order to justify the corporation's expenditures and the way its budget is managed with regard to a number of aspects—including travelling and meals. I just wanted to inform the chair, the clerk and the whole committee that this motion will be moved today.

The Chair: Thank you. You can submit your notice of motion to the clerk if you have it with you, and we can discuss it eventually, given the required 48-hour notice.

So, we will spend the first hour of our meeting discussing the two reports produced by the commissioner. The second hour will be used to discuss the main estimates.

I yield the floor to Ms. Stoddart for a ten-minute presentation on the two reports.

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

I want to begin by congratulating you on your recent election as chair of this committee.

[*English*]

Mr. Chair and honourable members, good morning. I'm very pleased to have the opportunity to speak with you first about the two annual reports that we lay before the House of Commons every year.

I'm joined here today by Assistant Privacy Commissioner Chantal Bernier. Madam Bernier is in charge of our day-to-day operations, and she's also a specialist on national security questions, so I appreciate her presence with me today.

I will focus my opening remarks largely on our public sector work, although there were certainly interesting developments on the private sector side as well. The principal focus of our annual report on the Privacy Act for the 2010-11 fiscal year was the federal government stewardship of the personal information of Canadians. In particular, we looked at privacy in the context of law enforcement and aviation security. The report examined whether departments and agencies collected, used, and disclosed personal information in a way that complies with the Privacy Act. This is of overwhelming importance, given the highly sensitive nature of so much of the personal data that the state needs in order to govern. Indeed, we're talking here about information related to people's income, their taxes and benefits, their travel patterns, and so many other aspects of their lives. This is not information that individuals would necessarily want to turn over. It is simply collected to fulfill the requirements of various government programs or activities.

In the main, I'm happy to say that we found that the Government of Canada has solid policies and practices in place to safeguard the privacy of Canadians, but we also said that the government is obliged to handle the personal information of Canadians with an uncompromising level of care, not some of the time or even most of the time, but all of the time. The fact is that over-collection, misuse, or inappropriate disclosure of sensitive personal information could carry grave consequences for individuals.

Our annual report summarizes two audits that our office conducted during the year. I'm going to summarize them briefly.

[*Translation*]

In terms of the auditing, we assessed whether the policies and practices of the Canadian Air Transport Security Authority, better known as CATSA, complied with the Privacy Act.

That audit concluded that the agency collects too much information about air travellers and does not always safeguard it properly. In particular, we found that CATSA collected personal data about traveller activities that do not relate to aviation security and that, in some cases, are perfectly legal and legitimate.

For example, CATSA will note when a passenger on a domestic flight is found to be carrying large sums of cash, even though there is no law prohibiting that. The over-collection of data is worrisome because it can result in undeserved suspicion being cast on an innocent person. In addition, our audit turned up gaps in the measures used to safeguard such records.

Indeed, in our spot checks of several major Canadian airports, incident reports were found on open shelving units and on the floor, in the same location where passengers are taken for further screening.

[*English*]

I'll talk a bit now about the RCMP audit. Our other audit looked at the Royal Canadian Mounted Police's management of two operational databases that are widely shared with other police agencies, government institutions, and other organizations.

You may have heard of CPIC, the Canadian Police Information Centre, and PROS, the police reporting and occurrence system. CPIC has been described as the backbone of the criminal justice system. It provides computerized storage and retrieval of information on crime and criminals and is widely used by the law enforcement and criminal justice community. PROS, meanwhile, is the RCMP's police records management system. It contains information on individuals who have come into contact with police, as a suspect, a victim, a witness, or an offender.

Our audit found that, in general, the RCMP has policies and procedures in place to properly govern access to and use of data in CPIC. However, one-third of the agencies that use CPIC were unable, for technical reasons, to implement the necessary protocols that ensure CPIC is accessed only by authorized users.

With respect to the PROS database, we also discovered that some outdated and erroneous personal information was being retained when it should have been sequestered or purged. Specifically, we found that police and other agencies with access to PROS could continue to view records related to cases that had resulted in a wrongful conviction or a conviction for which a pardon had been granted. This contravenes the data retention provisions of the Privacy Act. It also makes it harder for people to get on with their lives, free from the taint of unfair suspicion.

Both CATSA and the RCMP agreed to address our recommendations. We'll follow up to see how these recommendations will be implemented.

Our last annual report to you discussed follow-up work on three audits we conducted during 2008 and 2009. We wanted to see how many of the 34 recommendations we made in those audits had been implemented. We were happy to find that 32 of those recommendations had been fully or substantially implemented in the intervening years.

The results were, in some cases, significant. For instance, a follow-up to an audit on the RCMP's exempt data bank found that tens of thousands of surplus files had been purged to comply with our recommendations.

● (1110)

[*Translation*]

I will now turn to our 2010 annual report on the Personal Information Protection and Electronic Documents Act, the PIPEDA. The major issues in that report were online privacy and the disposal of personal information.

We highlighted our audit of a major retailer, Staples Canada Inc. —Bureau en Gros Ltée.

What we found was that Staples Business Depot stores fail to fully wipe customer data from returned devices such as laptops and USB hard drives, which were destined for resale.

That was a particularly disappointing finding, as we had already conducted two earlier investigations involving returned data storage devices at Staples and received assurance that the company would fix the problems we identified.

Although some steps have been taken, the audit showed that those procedures and controls were not consistently applied, nor were they always effective.

As a result, consumers' personal information was at serious risk.

At the end of our audit, we asked Staples to provide a report from an independent third party confirming compliance with the recommendations by the end of this June.

We look forward to hearing about how the company has addressed our recommendations.

[*English*]

The report also describes our investigation into Google's collection of highly sensitive data from unsecured wireless networks in neighbourhoods across Canada. The investigation found that Google's Street View cars had inappropriately collected personal information, such as e-mails, user names, passwords, phone numbers, and addresses.

Google's explanation for this serious violation of Canadians' privacy rights was that an engineer had developed code that included lines allowing for the collection of payload data, but failed to flag this to the company lawyer reviewing the project.

We were concerned about Google's lack of control over processes to ensure that necessary privacy protections were followed. We recommended that Google ensure it had a governance model in place to comply with privacy laws. We also recommended enhanced privacy training for Google employees.

There have been significant developments on that file since we published our annual report. Last year we examined the remedial measures Google had put into place following the investigation. We found the company was well on its way to resolving serious shortcomings. However, we did request that Google undergo an independent third-party audit of its privacy program.

We asked Google to share the audit report with our office within a year. We look forward to reviewing the results in the near future.

We've also started to use the approach of requesting third-party audits of companies with other organizations as well.

In conclusion, I've touched on only a very few of the many issues discussed in our two annual reports. I think both reports illustrate the very broad range of privacy issues that can have significant consequences for all Canadians, and the importance of having strong legislation in Canada to protect our privacy rights.

I thank you very much for your attention. I and any members of my staff who may be able to assist me look forward to answering your questions.

[*Translation*]

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

Mr. Angus has seven minutes to ask questions about your presentation.

[*English*]

Mr. Charlie Angus (Timmins—James Bay, NDP): Thank you, Mr. Chair.

Madam Stoddart, thank you for your excellent reports. In our business we read many reports. Often it seems reports are just data, but sometimes we come across a report like yours, which has a clear vision of the issues of privacy, the state's role, and the rights of the individual. I think it's a very powerful statement.

You state that security and privacy are not opposing values. You also state:

> ...the state also has an obligation to treat individuals with respect—to preserve their dignity and to safeguard their personal information.
>
> This is not a mere frill or a "nice-to-have"; it is fundamental to the trust relationship that must exist between citizens and their government.

I think that's a very clear and powerful manifesto with which Canadians would agree. The question is how to ensure that this trust relationship is not eroded.

I'm particularly concerned, for example, with Bill C-30 and the lack of protocols that will exist in terms of being able to collect and hold personal data. People have raised concerns about Bill C-30. I know that you've raised concerns. The minister, Vic Toews, said that people who raise concerns are on the same side as the child pornographers, which I find to be a very offensive statement about the issue of privacy.

What are your concerns about the lack of protocols in Bill C-30 to protect the privacy rights of citizens?

● (1115)

Ms. Jennifer Stoddart: Thank you very much for that question, honourable member.

In fact in the last few years we've been focusing increasingly on matters of national security and the maintenance of privacy rights because of the various new programs that have been developed.

We published a document that's available on our website called "A Matter of Trust", which sets forth the principles that we apply and that have been approved over the years within our country and by our courts, in terms of privacy principles and to the extent to which they have been respected. We hope that's a kind of blueprint or a series of suggestions for developing programs on the one hand and for telling Canadians what they can expect on the other hand.

In terms of C-30—in fact, I recently noted in going back over some material—I believe this was introduced under another name and title as far back as April 2009. So for not less than three years we have been commenting on this, both formally and informally. We've been meeting with department officials, and we remain very concerned with the architecture of the bill. Notably—and we have not changed what we've been saying for the last three years—it's with the ability to get personal information of Canadians without authorization, the fact that there is not a proper oversight framework, and that Canadians would remain largely unaware of what is going on.

While we do understand that technology and the access to very complex and efficient technology on the part of people who wish to do no good has complicated the work of our law enforcement forces in Canada, we think we need to see a clear explanation to the public to understand why new enhanced powers would be needed. Once that explanation has been done, we expect to see in any further iteration of the law—or we would hope to see—a more complete supervision framework as well as a role for independent authorization of access to personal information.

Mr. Charlie Angus: Thank you.

You state in your report that "Personal information is available...in unprecedented amounts, and the state's appetite for it is voracious." It's a very strong statement, so I think with the issue of Bill C-30 there's a concern. But the appetite of private companies for our personal information is equally voracious. I'm concerned about the protocols around how that privacy information is collected, and I see it from your audits of Google and Staples.

But I'm looking at Bill C-12 and the issue of security breaches and the provisions that exist right now—or the lack of provisions—and then the very loosey-goosey provisions the government is bringing in. If someone's data has been compromised, right now under this bill they say if there's significant harm they're obliged to tell the consumer. Significant harm seems to me to be an extremely high bar to set, given that a company is not going to really want to tell consumers that somebody was peeking at their data; they're going to quit the account.

How do you feel Canadians should be protected? Should the breaches be reported to you so that you can set the bar? Should we allow private industry to decide whether or not there's been significant harm? How do we ensure a balance? Is this something that should be reported back to you so you can make that declaration?

● (1120)

Ms. Jennifer Stoddart: Yes. That's another important question that my office is looking at. In fact, I've expressed my concerns with those parts of Bill C-12 that deal with data breach protection. I think in the time that we've been aware of the magnitude of the data breaches that are happening—both within Canada and outside of Canada—to Canadians' information as it circles the globe...we need stronger provisions in C-12.

I'm concerned if Canada does not set a higher bar—including looking at sanctions for companies that do not take necessary steps to protect personal information—we will have fallen well behind the actual practice in many American states, of countries abroad, like the U.K., where fines are imposed for data breaches. They're mostly to public sector organizations, it seems.

I think we have to send a strong signal—and I sent this a year ago to companies—that data breaches are not acceptable. Some may be almost unavoidable because of the cutting-edge technology and so on, but many just seem to be lack of attention, lack of training, and lack of investment in data breach procedures and equipment.

[*Translation*]

The Chair: Mr. Angus, unfortunately, your time is up.

I now yield the floor to Mr. Del Mastro for seven minutes.

[*English*]

Mr. Dean Del Mastro (Peterborough, CPC): Thank you, Mr. Chairman.

Thank you to the witnesses today for very interesting testimony.

I was interested in the statement you made with respect to CATSA. Whenever I talk to law enforcement—and CATSA certainly is a law enforcement agency—what they indicate to me is that the more information they have, the better. They'll never turn down information; they will collect every piece of information they can get.

My question for them is why they need this. You said they were over-collecting data. What was their stated rationale for this? Did they have one? Did they have a reason for why they were asking questions that they weren't actually duty-bound to ask and collect?

Ms. Jennifer Stoddart: I don't think so, Mr. Chair, but could I ask Assistant Commissioner Chantal Bernier, who is closer to the details of that audit, to answer your question?

Ms. Chantal Bernier (Assistant Privacy Commissioner, Office of the Privacy Commissioner of Canada): Thank you.

Indeed, the relationship we have with CATSA is excellent. In this audit, when we did put to them that finding, they accepted to change the practice, recognizing that indeed they did not need that information, that it was beyond their mandate to collect it.

Mr. Dean Del Mastro: So it really was a situation where if they could get it, they'd take it, whether they needed it or not.

Ms. Chantal Bernier: Yes.

Mr. Dean Del Mastro: Okay.

You indicated that only one-third of the users of CPIC were meeting the required privacy guidelines. Is that as a result of, for example, small-town police stations and so forth not having the resources, or is it their not really understanding what their responsibilities are with respect to privacy, or some combination? What did you find with respect to the non-compliance with respect to privacy and CPIC?

It would seem to me CPIC should be pretty closely guarded.

Ms. Jennifer Stoddart: Yes, you're absolutely right. But with the range of organizations across Canada that are attached to CPIC, I don't know if there's one simple response. I don't know if the assistant commissioner does. We have the head of audit and review, if you'd like to hear the answers that were given back.

We're talking about people who plug into CPIC who are not necessarily under federal jurisdiction—municipal or provincial police forces. So I don't think it was really our business to go and say.... We did CPIC and we noted with some concern that a third of those accessing CPIC didn't have designated users.

Mr. Dean Del Mastro: So it's a third that are non-compliant, not a third that were compliant.

Ms. Jennifer Stoddart: Yes, a third were non-compliant. That's my understanding.

Mr. Dean Del Mastro: It's still a significant number. You're talking about a significant number of people who are using that system who aren't meeting guidelines for the use of it.

Ms. Jennifer Stoddart: Exactly. It wasn't the RCMP; it was those that are partners with the RCMP, which may be much smaller organizations.

● (1125)

Mr. Dean Del Mastro: Okay, thank you.

I'm pleased that 32 of the 34 recommendations that you made previously were fully or substantively instituted. That's good news.

I'm also pleased to hear that Google is cooperating so well. I'm not meaning to give props to Jacob Glick and Google here in Canada, but I can't remember the last time I used another search engine online. I'm glad to hear that they're returning the loyalty that Canadians have extended to them with a cooperative spirit. That's good to hear.

I wanted to ask another question. Mr. Angus talked a little bit about Bill C-30. I know that's not what you're here specifically to address. Of course, notwithstanding the fact that I don't believe Canadians should be providing any more information than what they absolutely are required to by law, I think...as you said, governments have a duty to protect that information; they require it for the operation of government. At the same time, I'm always concerned that there is an element within society that uses rules like privacy laws to hide illegal activity, to hide themselves amongst otherwise law-abiding citizens, and to use those protections that we fight for, that I think all parties fight for and have always fought for. They utilize those protections, those privacy laws, to do criminal acts.

It's never going to be easy to determine...and I think it's true to say there are sacrifices we all must make in order to make sure our law enforcement officers and so forth have the ability to track down those who would otherwise seek to exploit our privacy laws to break the law. You talked about having a conversation with Canadians—I'm paraphrasing—to justify why these changes need to be made. Have you been approached by groups or police and law enforcement that have talked to you about some of that rationale, about some of the things they're seeing? My local police chief came and talked to me, and it was very disturbing what he indicated to me about the challenge they're having tracking down, specifically, people who are trafficking in child pornography.

Ms. Jennifer Stoddart: Thank you. These are really important questions and important concerns.

If I may, Mr. Chair, I'll ask Assistant Commissioner Chantal Bernier, who has a background in national security and can answer that better than I can....

Ms. Chantal Bernier: Indeed we agree with you that privacy cannot stand in the way of public safety and cannot be used to shield illegal activities. That is our starting point. We have consulted widely, I would say, with chiefs of police, the RCMP, and CSIS, as well as with civil society, to truly make the distinctions that are appropriate in consideration of this legislation.

The commissioner earlier referred to the document called "A Matter of Trust". You would find if very helpful, I believe, in that it puts forward an analytical framework, precisely to make the distinctions that you suggest must be made.

That analytical framework calls, first of all, for empirical evidence of the need for certain powers that do indeed call for breach of privacy in certain circumstances. Secondly, it calls for the justification to keep the personal information that is collected, and then of course an oversight mechanism to ensure that all the rights that must be upheld are upheld.

[*Translation*]

The Chair: Ms. Bernier, I have to ask you to wrap things up in 15 seconds.

[*English*]

Ms. Chantal Bernier: So the bill must be looked at through that lens, to precisely ensure that it only targets those who must be targeted and therefore avoid using privacy as a shield for illegal activities.

[*Translation*]

The Chair: Thank you very much.

I want to let the committee members know that the report titled "A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century", which Ms. Bernier mentioned, is available upon request. The clerk will provide you with an Internet link, so you can access that report.

I yield the floor to Mr. Andrews for seven minutes.

● (1130)

[*English*]

Mr. Scott Andrews (Avalon, Lib.): Thank you very much, Mr. Chair.

Welcome, ladies, to our committee this morning.

During your opening remarks you talked about the over-collection of data. How common is that? There's the one example you gave, but how common would it be across government that some government departments probably do an over-collection of data? Is this something we should be concerned about in some other departments as well?

Ms. Jennifer Stoddart: That's very difficult to say, across the government. I would say it's kind of a natural tendency. I think one of the honourable members referred to the fact that staff always want to get more information to make sure they're doing the right thing, and that they administer programs and so on. I think a lot of it is extremely well intentioned, but it may not be necessary. As the assistant commissioner said, you have to justify why you collect personal information from people, conceptually and in terms of the Privacy Act.

So what we do is.... The Treasury Board asks organizations that are setting up programs where personal information will be collected to do privacy impact assessments. They're often known as PIAs. It varies by year; we have anywhere from between 60 to 100 PIAs that are sent to us. We don't review all of them. We don't have the resources for that. We review the most significant ones, and then we try to whittle down the over-collection of personal information, where that happens.

Mr. Scott Andrews: Are these PIAs common practice? From your experience and from what you've seen, is that being done in all appropriate circumstances?

Ms. Jennifer Stoddart: I don't believe it's 100%, but I'd say it's for the majority of programs with personal information, especially the ones with sensitive personal information.

The assistant commissioner talked about our work with CATSA. We worked very closely with them on the development and implementation of the body scanner and so on.

So in the majority of cases, yes, it is done.

Mr. Scott Andrews: Do you work with the different departments on the disposal of that information? At what times do they have to dispose of the information or provide safe disposal of the information? Is that a concern at all?

Ms. Jennifer Stoddart: It is a concern, honourable member. One of the audits we did recently showed there were huge problems in the disposal of information by the targeted agencies.

We audit disposal practices from time to time. We remind departments of their obligations, for example, in Industry Canada, to wipe computers clean before they give them to schools, or, in the case of Library and Archives Canada, to make sure the contractor who's shredding the information is actually following the standards of the contract. As I said, then we do a follow-up in the next two or three years to see that the recommendations are being implemented.

Mr. Scott Andrews: When you were talking about Google, you mentioned third-party audits and other organizations. What other organizations would you be referring to, like Google, that consumers should be aware of?

Ms. Jennifer Stoddart: Under the terms of both acts, I can't name or talk about in detail ongoing operations unless it's in the public interest.

What I'm referring to is a new position I've taken in the last year because I'm concerned about the cost of enforcing privacy that is borne by the taxpayers of Canada. I think when we come to the end of an investigation and the company has not worked with us to resolve the problem and is still saying they don't care and they're not going to do anything, or they say they were in the wrong and they're going to do something, we should not as a government agency have to go back and audit them. That costs people and time and so on. So from now on, we're adopting a practice that, for example, is frequent with the Federal Trade Commission, one of our American counterparts. If you have real violations of the Privacy Act, PIPEDA in this case, we ask you to go and get a third party to verify that you've fixed it up and sent that back to us.

Mr. Scott Andrews: I'm sure you are familiar with, and have seen in the media, the robocalls scandal and the information of voters being given to parties to do other things with.

I understand that political parties don't fall within the guise of a lot of data protection and what they do with their data. Have you been following this file at all? Do you have any suggestions on how political parties could better secure their data?

● (1135)

Ms. Jennifer Stoddart: I think I would wait until the director general of elections has finished looking into this. But certainly in the past we have met with various members of Parliament, different parties, and we've also developed material on helping MPs secure the personal information of many of the voters they represent.

Mr. Scott Andrews: I have a question on Bill C-30. Your counterpart in Ontario, Ann Cavoukian, has been quite critical of Bill C-30, and she's been quite vocal. Do you share some of her comments regarding Bill C-30?

Ms. Jennifer Stoddart: As I mentioned, we've been following this for three years and have done a lot of substantive work that we have shared with provincial and territorial privacy commissioners. That's why we could together take a position on it. I think there's a common viewpoint among privacy commissioners across Canada.

Mr. Scott Andrews: Thank you.

[*Translation*]

The Chair: Thank you, Mr. Andrews.

Mr. Butt, you have the floor for seven minutes.

[*English*]

Mr. Brad Butt (Mississauga—Streetsville, CPC): Thank you very much, Mr. Chair. I don't think I had a chance to say at the last meeting congratulations on being elected the new chair of the committee.

Madam Commissioner, thank you very much for being with us this morning. In your report you stated that the number of visits to your website has increased by 36% from the previous year. How do you explain that increase? Maybe that's a positive thing because public awareness is much higher. How does the situation influence the information you are then placing online?

Ms. Jennifer Stoddart: Thank you for your question.

We have made a conscious attempt to develop not only our website but also a youth website. We have a youth blog. We have increasingly invested in online information as Canadians and young people are increasingly online, as compared to reading written material or even watching TV. This is a very good development for us, because in an age when resources have to be counted very carefully, we think that's a very cost-effective way of getting the message out to Canadians.

Mr. Brad Butt: My daughters are 12 and 8, and my 12-year-old is tweeting and texting and all kinds of other stuff now. We obviously remind her and warn her to protect her privacy and to be a responsible user, but I am concerned about people's privacy because of the way the Internet and all these other social media sites and so on have evolved. It must make your job increasingly difficult, to draw those distinctions in what should be protected through privacy and what is really there for public consumption.

Are you finding it more difficult to draw some of these conclusions when you're investigating different things, just based on the fact that things are evolving so rapidly online? Are there additional tools you may need to react to the fact that this is the way the world is evolving?

Ms. Jennifer Stoddart: It's a very good question.

In the time I've been Privacy Commissioner, which is a little over eight years now, yes, things have evolved tremendously. The pace at which we have to rethink and reposition ourselves has just increased exponentially.

All over the world people are looking at what the definition is of "personal information", what should be public and private, and of course at the same time you have the parallel discussion about open government and all of those developments.

I don't know that there's any one resource that would help us. This is part of our work, but certainly one of the places where we've invested in the last few years is setting up our technology analysis branch. The director is here, if you would like to hear more about what that branch does. And there are six or seven people who are very specialized in information technology who analyze mainly what happens on the web, what's happening with mobile apps, what the implication is, and they advise us on our investigations.

● (1140)

Mr. Brad Butt: The second area—if I still have some time, Mr. Chair—I want to quickly touch on is PIPEDA and the parliamentary review that I guess will be taking place imminently.

I remember back before I got to this place, when I was the president of the Greater Toronto Apartment Association. We actually helped our members develop a standard privacy template because they were collecting personal information on their tenants living in apartment buildings.

I'm quite familiar with the rules around PIPEDA and some of the pros and cons of that, and obviously some of the administrative difficulties that does create for some private sector companies that are collecting personal information.

How are you preparing for that review? Do we have any timelines as to how we're relooking at that and what role either Parliament needs to play or what role you are simply playing within your own office to deal with the whole protection of privacy and electronic documents act?

Ms. Jennifer Stoddart: We have been preparing for the next PIPEDA review for the last three years. We will have completed our final positions, I'd say, by this summer, so I am very interested in your question. I'm really hoping that Parliament will look into PIPEDA. The last review was in 2006, I believe, by this committee.

We are, I guess, a little past due to look at PIPEDA again. We've had some major work done by some law professors. We have complementary work done. We have a lot of developments that have happened in organizations that are like ours in other countries, things coming out of the United States, out of Europe, and so on that I think should inform a review of PIPEDA now. So we're looking forward to that.

Mr. Brad Butt: Okay.

Is that it, Mr. Chair, or do I have more time?

[*Translation*]

The Chair: Mr. Butt, you have a minute and a half remaining.

[*English*]

Mr. Brad Butt: Have you identified any specific areas around PIPEDA that you would be recommending be improved in the legislation, changed, deleted? Are you at that stage yet, where you have semi-ideas around what you might be recommending to us should there be a formal review of the legislation?

Ms. Jennifer Stoddart: Yes, certainly we're looking at enforcement issues. There are some technical issues that have come up in previous work, but certainly enforcement is a major topic for consideration, because as you know now, there's an investigation, and if the alleged victim, the complainant, consents and the case is not resolved, we can go to the Federal Court.

In the Federal Court there are no statutory damages, and this differs from the privacy regimes now in comparable countries. People who have suffered some harm in the Ontario Court of Appeal spoke to this recently in a case. There should be some recognition of the harm they've suffered.

Strengthening the enforcement regime, I would think, would be something that should be considered at this point. There has to be some kind of sanction, on the one hand, for companies that don't pay attention to privacy, and on the other hand there has to be some recognition that if this is an important value, well, people should be compensated.

[*Translation*]

The Chair: Thank you. Your time is up.

Ms. Borg, the floor is yours for five minutes.

Ms. Charmaine Borg (Terrebonne—Blainville, NDP): Thank you, Mr. Chair.

I want to thank Ms. Stoddart and Ms. Bernier for joining us today.

Ms. Stoddart, when you talked about CATSA, you highlighted a problem regarding protocol compliance by private companies with contracts for passenger screening. You mentioned certain gaps in their methods of data disposal and incident report safeguarding. In Bill C-30, the reliance on private companies to collect and safeguard personal information is apparent. Are you concerned by this increased reliance? Is that a current trend?

Ms. Jennifer Stoddart: I will ask the assistant commissioner to answer your question.

Ms. Chantal Bernier: Exactly. Public-private partnerships have an impact on privacy. Continuity must be established in the protection of privacy, and that continuity must be ensured through a strong and effective legislative framework.

In CATSA's case, that contract ensured that the agency's obligations with regard to privacy also applied to subcontractors. Therefore, this violation of privacy was non-compliant, and it violated the Privacy Act.

CATSA acknowledged the fact that it needed to improve its monitoring of contractors when it comes to privacy. Therefore, we expect improvements in the overseeing of contractors. Regarding your more general question, you are completely right. In our opinion, the public-private partnership phenomenon has very relevant repercussions on privacy protection, and we are monitoring the situation.

● (1145)

Ms. Charmaine Borg: Thank you.

My second question is about sections 3.1 and 3.2 of your report.

You say that a complaint by a former soldier prompted you to undertake an investigation into the Department of Veterans Affairs. In 2012, personal information regarding Thomas Hope, another veteran, was made public without his consent. I think that you are currently looking into that issue. Could you tell us about how you are monitoring that situation?

Ms. Chantal Bernier: There are a number of things that need mentioning. First, we have received several complaints. Therefore, we have several ongoing investigations. Second, following the first complaint, we noted some systemic deficiencies or an appearance, at first glance, of such deficiencies in the management of personal information at the Department of Veterans Affairs. That is why we decided to conduct an audit. So we also have an ongoing audit, which should lead to a report that will be submitted to you in the fall.

Ms. Charmaine Borg: To follow up on this last question, I am worried by the fact that there have been so many violations of access to personal information involving veterans. Another one of my worries is that this may also be happening in other departments.

There is an increasing number of government services that are, in some cases, available only on line. Is that a reality we must get used to? Does that worry you?

Ms. Jennifer Stoddart: Indeed, the idea of potential technological problems or programming errors is worrisome. One of our annual reports talks about such a case. On a Service Canada website, personal information on a number of individuals was suddenly exposed.

We are talking to the government about the security standards needed to establish new steps for providing Canadians with access to an online government. This is still an area we monitor carefully, and we hope that the government will continue to do so as well.

The Chair: Thank you, Ms. Borg.

Mr. Mayes now has the floor for five minutes.

[*English*]

Mr. Colin Mayes (Okanagan—Shuswap, CPC): Thank you, Mr. Chair.

I welcome our witnesses.

One of the aspects that you've touched on a little is that, really, communications and issues of privacy are not just domestic issues; they're international issues. Do you work with agencies internationally to see the best practices and legislation they have and model the best of the best...? Could you give me some examples of that, please?

Ms. Jennifer Stoddart: Yes, absolutely, honourable member. It has been clear for many years now—and I've always said this to the committee—that the nature of privacy online now means that privacy is an international issue.

One of my own personal focuses, and the focus of Canada when we take part in international organizations like the OECD, is to encourage cooperation and the emergence of standards that can be shared among different groups when we're faced with the doings or the developments of international companies like some that we've met here. For example, there's the EU on the one hand, the U.S. on the other hand, and then Canada, New Zealand, and Australia, which are to the side. I believe that in our annual report we give some examples.

This continues to be a very important focus for my office, because often we have to coordinate—we're a member of something called the Asia Pacific Privacy Authorities—for example, on what Australia is doing, who's going to speak for us, and what the position of Hong Kong is when faced with the same phenomenon. But if you don't do that, then you're not providing effective privacy.

● (1150)

Mr. Colin Mayes: At one of the other committees I'm on, there was a representative from RIM, Research In Motion, and this question was asked: what does the future hold for RIM? He said that so much of your information will be on your BlackBerry, such as your driver's licence and maybe your passport.... There's a number of issues.

Do you have the resources to work with those who are developing those types of technologies, and to be able to work with them, so that you can see those safeguards they would apply as they develop these services within the products they produce?

Ms. Jennifer Stoddart: I think that now, with our technology analysis branch and the laboratory that we have developed, we have a lot of high-level, senior information technology people who have the contacts and the know-how necessary to communicate with companies like RIM. Of course, we don't have the resources to embed somebody in Google or RIM, even if it were possible, but I think our people make those companies aware of what our requirements are.

On that front, could I just mention that we're developing a mobile privacy app? I'm not sure what this is going to look like. It sounds pretty innovative to me. That is one of the projects that we hope to release to deal with the issue of what we're now all carrying on our mobile devices.

Mr. Colin Mayes: One of the issues I have is not just information, but incorrect information. I have constituents who say that they've come across the border, CBSA has somebody with the same name who is red-tagged, and then they are detained for five hours. They're very upset about that whole issue, and they ask why CBSA can't get this right.

Do you do any investigations about making sure that the information they have is correct information? Is there an appeal process that you oversee or that you ensure is in place, not only to protect privacy but to make sure that the information that is taken is the correct information?

[*Translation*]

Ms. Jennifer Stoddart: May I ask the assistant commissioner to tell us more about this?

[*English*]

Ms. Chantal Bernier: Absolutely, and that's one of the reasons why we need to pay particular attention to the work being done on the border security perimeter.

As for what we do in relation to the possibility of inaccuracy, first of all, our audits are done on a risk basis. So we will look at either the number of incidents or the volume and sensitivity of the personal information held by an organization to decide whether we should go in and do an audit.

Certainly, a high level of inaccuracy, or the high impact of possible inaccuracy, would be exactly at the root of deciding to do an audit, hence our audit of CPIC and PROS. This fits exactly into your question.

Indeed, CBSA is another organization that we work very closely with, because, as you mentioned, the impact of inaccurate information at CBSA is quite significant. So yes, that is the kind of monitoring we do.

[*Translation*]

The Chair: Thank you. Unfortunately, your time is up.

We will have to adjourn the meeting for a few minutes and then move on to the study of the main estimates.

Additional time will be allocated for questions on the main estimates. That may also concern many of the topics we just talked about.

We will adjourn the meeting for two or three minutes and will resume shortly.

Thank you.

● (1150)

(Pause)

● (1200)

The Chair: We will now continue our work on the study planned for the second hour of our meeting. I call vote 45 under JUSTICE. We will have a 10-minute presentation.

I will repeat for everyone. I call vote 45 under JUSTICE.

If Ms. Stoddart is ready to begin, she has 10 minutes for her presentation.

Ms. Jennifer Stoddart: I am ready, Mr. Chair. Thank you very much.

[*English*]

Honourable members, Mr. Chairman, I'm very pleased to be able to have a second hour with you to talk about some of our key priorities now for the coming year. We go into the future, having done the annual reports, and once again will attempt to answer your questions.

For this particular phase, I'm joined not only by the assistant commissioner, whom you've already met, but also with Daniel Nadeau, our chief financial officer and director general of corporate affairs. We were very pleased to have him join us in August, following the retirement of a gentleman some of you may have previously met, Tom Pulcine. It's been a wonderful, seamless transition. I'm very happy that Daniel is with me today.

I would like to begin by explaining the evolving landscape of privacy issues and how public concern with them affects our office's work and choice of priorities. So for starters, as I think everyone around this table can appreciate, personal information protection is an issue of growing importance here in Canada and around the world. Canadian businesses need to be informed about how privacy law applies to their operations, and federal departments and agencies are constantly challenged to balance social benefits associated with initiatives that gather personal information on the one hand with the privacy rights of individuals on the other. As an agent of parliament, my office, of course, has the task of advising on such issues.

Individuals today face a reality of complex information technology. People enjoy the fact that these tools connect us like never before, and they bring valuable services to our fingertips. At the same time, Canadians fear the consequences of being tracked by data mining marketers and being surveyed by governments. As a result, Canadians turn to us to investigate their complaints and for information to protect and assert their rights.

[*Translation*]

I will now talk about the key areas of the OPC's mandate.

As you know, our office is mandated with overseeing compliance with both the Privacy Act, which applies to the government, and the Personal Information Protection and Electronic Documents Act, which applies to the public sector.

We also provide guidance to organizations on the application of privacy law, and to individuals on how they can protect themselves and assert their right to privacy. As in past years, we will be pursuing these objectives through actions under the following three key areas: compliance activities, research and policy development, and public outreach.

Before we get to your questions, I would like to highlight some of the key priorities we are pursuing over the coming year for each of those areas.

[*English*]

First of all, I'll start with compliance activities, where we are continuing our work to update and strengthen our complaint intake and investigation processes. In particular, we are in the midst of an effort to develop and adopt more innovative practices in the Privacy Act investigation process. Our goal is to continue resolving complaints thoroughly with a view to providing service to Canadians in a more efficient, effective, and timely manner.

We are also taking action to better deal with the fact that an increasing number of privacy issues are tied to information technology. For this reason, we are taking steps to ensure that we have the right expertise and tools to evaluate the privacy impact of various technologies. On top of improving ways to do our existing work, we are also focusing on the best approach to fulfilling new responsibilities.

As you know, it's expected that Canada's anti-spam law will come into force sometime next year. We are working alongside Industry Canada, the CRTC, and the Competition Bureau to develop the processes and systems to fulfill our respective roles under this legislation.

In addition, we're also gearing up to review the privacy impact assessments tied to the many initiatives being developed across government, to realize the vision outlined by the Canada-U.S. perimeter security and economic competitiveness action plan. Our office and our provincial and territorial counterparts have underlined the fact that many of the planned initiatives in this plan contain privacy risks.

Our office is ready to examine the assessments to come in order to make recommendations to departments on how to mitigate such risks. With respect to audits, as the assistant commissioner said, we will lay before you the audit of Veterans Affairs Canada this fall, and we have just commenced our second mandated audit of FINTRAC.

● (1205)

[*Translation*]

I will now discuss research and policy development.

As an agent of Parliament, we will continue to devote our expertise to analyzing legislation and sharing our observations with parliamentarians. We will also be paying special attention to the upcoming parliamentary review of the private sector act. That review is mandated every five years—and for good reason, as we have already mentioned.

Another way we help meet Canadians' privacy needs is by working with leading academic researchers in the field. One important way we do this is by supporting independent, non-profit research through our Contributions Program. Over the course of this year, we look forward to supporting further research, which can lead to new ideas and insights on privacy protection issues.

[*English*]

I'll talk now a bit about public education.

Public education is vital as privacy issues continually evolve. Very few of us can grasp the technological intricacies of what's happening on the other side of the screen. It's therefore more and more important I think to assist Canadians in protecting their personal information online. The generation growing up today is really the first to grow up online. This is why our outreach efforts to youth, to parents, and to educators remain among our top public education priorities.

We've already developed presentation materials for grades 7 through 12 to help adults engage youth about the privacy challenges of today's online world. This year we will be promoting education materials for grades 4 through 6. In addition to individuals, we know that businesses, especially small ones, have specific needs. In general, small businesses lack the resources to have dedicated in-house chief privacy officers and legal counsel. As a result, we're dedicated to providing guidance materials and making outreach efforts to help small businesses learn about and comply with their privacy obligations. Included as part of this we will be spreading the word about the importance of cyber-security and the steps small businesses need to take to protect customer and client data in the online age.

In relation to the public sector, significant changes in our public safety context, as well as in government interaction with citizens online, call for us to educate Canadians on the privacy implications of measures resulting from these changes.

In closing, Mr. Chair, let me underline that we will carry out our work in a way that will continue to see Canadians both well respected as taxpayers and well served as citizens. While not mandated to make reductions under the deficit reduction action plan, our office answered the call to adhere to the exercise's spirit and intent. As a result, we proposed to the government that we would find savings of 5%, or $1.1 million per year, within our operations by fiscal year 2014-15, while maintaining the best possible level of service for Canadians. This proposal was accepted and reflected in our budget for 2012.

To deliver on this, we have planned the following reductions: $676,000, or 2.8%, starting this year, will come from funding that had been allocated to my office in support of the implementation of the Federal Accountability Act. This funding was never accessed by the Office of the Privacy Commissioner. Then, an additional $430,000, or some 2.2%, starting in 2014-15, will be absorbed through general efficiencies from across the organization. Efforts to improve the use of technology and available tools, to take on a greater risk management approach, to better target public education activities, and to seek out partnering opportunities will help OPC generate these savings.

In addition, I also want to note a looming cost pressure that poses a challenge to our quest for a workable balance between quality services and lower costs. A forced move out of the OPC's present location to new offices in 2013 will result in additional costs of up to $5 million. Right now we cannot absorb this without significant impact on our core program. We're currently negotiating with the Treasury Board Secretariat to address this pressure, and I'm hopeful this issue will be settled adequately in the very near future.

● (1210)

With that, I look forward to your questions. Monsieur Nadeau will help me with any detailed questions on our finances.

[*Translation*]

Thank you very much, Mr. Chair.

The Chair: Thank you for your presentation.

I now give the floor to Mr. Boulerice for seven minutes.

Mr. Alexandre Boulerice: Thank you very much for this presentation and the one you made during the first hour, Ms. Stoddart.

I am a bit worried after hearing the last part of your presentation regarding the financial pressures imposed by the budget cuts the Conservative government introduced. That will affect your ability to act and to carry out your growing number of tasks. Your tasks are multiplying, while your means are decreasing. I don't know how you will deal with that. It's a concern for all Canadians.

I want to come back to a specific issue. We are officially on the Department of Justice's vote 45, but I want to take a few moments to emphasize the fact that, if we rely on this document regarding expenditures, your budget is increasing. It is going from $20 million to $22.129 million. We also know that this document has nothing to do with the budget, which is calling for a reduction in spending.

You just said that you suggested a 5% budget cut and that, among other things, you will move, you will be more efficient and will better target public education activities. What do you mean by "better target"? Does that mean that you will provide fewer public education activities, even though more are needed?

Ms. Jennifer Stoddart: No. In answer to the last part of your question, I would say that we will use virtual tools more extensively. As I already told another member of the committee, I believe that virtual tools are less expensive and are probably increasingly efficient. We will try to be more careful about choosing audiences we think will benefit the most from our efforts. For instance, we will prioritize young people.

Mr. Alexandre Boulerice: Thank you.

In this current climate, a sword of Damocles is hanging over our heads. I am talking about Bill C-30, which the government wants to use to provide the Competition Bureau, the Canadian Security Intelligence Service and law enforcement agencies with direct access to personal data through Internet service providers. I have a feeling that will increase your workload considerably.

What kind of consequences do you think pieces of legislation such as Bill C-30—which enables Internet providers to directly search Canadians' computers—will have on your work, in terms of protecting personal, private and confidential citizen data? In addition, considering the cuts to your budget, how will you deal with that type of situation?

Ms. Jennifer Stoddart: Bill C-30 does not give us any specific additional roles. If my memory serves me correctly, the bill mentions that we can conduct audits, but we can do that anyway. What we're worried about is the overall content of the bill. Since the bill is currently being discussed and the same issues have been raised for three years, our efforts are currently focused on the final version of the bill. For 10 years, various versions of this bill have been introduced, so we will have to wait and see. If the bill does not give us a specific role, the consequences of this new expenditure restraint program will clearly carry a lot of weight in terms of the risk elements that lead to audits, given our current resources.

Mr. Alexandre Boulerice: This bill is always a topic of discussion, but what kinds of difficulties or challenges do you think are involved in its current version? Should Canadians and Quebeckers worry about their privacy being jeopardized?

● (1215)

Ms. Jennifer Stoddart: I think we have clearly emphasized for a long time that this bill was unacceptable in terms of protecting Canadians' personal information and privacy. There are no safeguards or appropriate procedures to compensate for the infringement upon Canadians' privacy, to which police services have fairly direct access.

Mr. Alexandre Boulerice: Thank you.

I know we are talking about the future, but sometimes you need to look back at the past. A few years ago, you performed an audit of the RCMP's database, and you came to the conclusion that it was mismanaged. It appears on page 41 of your annual report. Consequently, you forced the RCMP to get rid of all excess and unnecessary data. That represented about 95% of the information.

How will you ensure that, going forward, other departments will not do the same and collect unnecessary information on Canadian citizens, particularly in this climate of fiscal restraint?

Ms. Jennifer Stoddart: I will let the assistant commissioner, who is responsible for national security issues, answer that. She will be able to respond in more detail.

Ms. Chantal Bernier: As you pointed out, that audit led to the destruction of all data that did not need to be kept. I would say that speaks quite nicely to the effectiveness of our audits and the receptiveness of federal agencies, to be sure. That being said, it is necessary to keep up that oversight. As I was explaining earlier, we have a risk-based audit plan, where we determine which organizations to audit according to the volume or nature of information they hold and the number of incidents.

That is how we ensure that irrelevant data is not kept unnecessarily.

Mr. Alexandre Boulerice: Mr. Chair, I see you are telling me I have only a minute left, so I will keep it short.

Ms. Stoddart, you said that you were going to expand your use of online services, which are more cost-effective, to reach young people and so forth. I am in favour of that. As politicians, we use them in our ridings. But I see a contradiction of sorts. Are you going to use Facebook to warn young people about the dangers of Facebook?

Ms. Jennifer Stoddart: No.

Mr. Alexandre Boulerice: Young children are not supposed to use Facebook. As a parent, I find it incredibly worrisome. In your view, what are the risks associated with Facebook, Twitter or MySpace for our children and young people, aside from cyberpedophiles, which I can well imagine. What risks do our children face when it comes to these new social media networks, and how are you going to warn them about the risks?

Ms. Jennifer Stoddart: Very well.

The Chair: You have about 30 seconds to answer.

Ms. Jennifer Stoddart: Okay.

First, we are doing more work with institutions that have relationships with school boards to give teachers tools, and that is happening across Canada. Second, young people have trouble imagining all the possible repercussions, given the complexity of how these sites are designed. It isn't always obvious that when you share something with everyone, you really are sharing it with everyone, not just your friends and such.

So, for us, trying to force social networks to provide clear explanations so that young people using their sites can more easily understand what is involved is a never-ending battle, because these sites change almost daily. It is incredibly hard work.

The Chair: Thank you for your response.

It is now over to Mr. Dreeshen for seven minutes.

[*English*]

Mr. Earl Dreeshen (Red Deer, CPC): Thank you very much, Mr. Chair. Again, I congratulate you on your position.

To Madam Stoddart and our other witnesses, thank you so very much for coming.

When I was first elected in 2008, I was on the ethics committee, and I've had an opportunity to address you on other occasions. Of course, as a former educator, I think it's part of what you were talking about here, that public education is so important. It's great to see that you've moved that awareness into grades 7 to 12, and it is necessary to make sure you get into the lower grades as well, to make sure they understand just what is taking place. You also have the situation of education being twofold. It is not just for our youth but also for businesses, so that they understand what is taking place.

I note in the report that you talked about a 30% decline from the previous year in inquiries related to the Privacy Act. The number of visits to the Office of the Privacy Commissioner website is up by 31% from 2007-08 to 2.2 million visitors in 2010 and 2011. I'm just wondering if we could tie that into the educational component of the activities you have been doing in your office.

● (1220)

Ms. Jennifer Stoddart: I think, honourable member, that's a very plausible explanation. We don't always know ourselves why there are more complaints or fewer complaints and so on.

Just recently, complaints from the private sector have been going up, as have, I believe, those from the public sector. We're asking ourselves why this is. Hits to the different websites have been going up. I think that's possibly in relation to a lot of the discussion around Bill C-30 recently. Canadians are very concerned about their privacy rights.

Mr. Earl Dreeshen: That's very good.

The other things—and you talk about this on page 86 of your report—is on the most common complaint types that are received, and it looks as though access is the main one. We're talking about 46% of the complaints being about access, 36% about time limits, and 18% about actual privacy. I wonder if you could expand on that.

Ms. Jennifer Stoddart: Is this in the public sector act?

Mr. Earl Dreeshen: This is in the Privacy Act on page 86—the percentage breakdown.

Ms. Jennifer Stoddart: On complaints respecting the government, the key issue has always been, "Can I get access to my personal information?" or "If I have access, I don't believe it's everything." We know there are very few Canadians in public security files who don't have access to their personal information, for allowable reasons. This is distinct from the private sector, where it's the use of personal information. Sharing with other organizations is the main subject of complaint.

On time limits, it's almost 40%. This is a very specific issue, and I wonder if it is a very useful part of the law in this day and age. It allows a person whose request has not been answered in 30 days to make a complaint. This is overwhelmingly used by people who are incarcerated. We then work with them to resolve the complaint and the substance of the complaint. Correctional Service Canada is a big subject of complaints. But I don't know if that mechanism is as efficient now in 2012 as it was when the act was initially drawn up.

Mr. Earl Dreeshen: That looks as though it is a cost driver that you have. Of course, we're trying to look at the dollars associated with the organization.

I'd like to go back to another discussion we had in the past on your staff. There was a concern earlier about your staff turnover. I wonder if you can comment on whether that has stabilized and what you see going forward.

Ms. Jennifer Stoddart: Yes, thank you.

When I became Privacy Commissioner I tried to rebuild the office. I know in this committee we have talked about staff turnover for years; however, I think that turnover has stabilized. We've been able to recruit, and we sometimes have very long recruitment processes because many of our people....

One of the honourable members asked how we deal with this, given that it's becoming more and more complex. We have to hire more and more expert people. But we have very qualified staff. We have a stable workforce, and I believe we'll be able to keep all of them in the years to come.

Mr. Earl Dreeshen: The next question I have has to do with the anti-spam bill. It received royal assent at the end of 2010. You stated in your report that the legislation will result in important changes to your office. I wonder if you can elaborate on those changes.

● (1225)

Ms. Jennifer Stoddart: We have a new responsibility around the illegal harvesting of e-mail addresses. This has already precipitated, without the law coming into force, intensive discussions with Industry Canada, the CRTC, and the Competition Bureau. They have bigger roles in the overall anti-spam legislation than we do.

Mr. Earl Dreeshen: Does that seem to be working well? You aren't having any difficulties there and it is working as smoothly as you had anticipated?

Ms. Jennifer Stoddart: I think it's progressing along.

Perhaps I will ask the assistant commissioner, who is in charge of operations, to tell you about a program we're organizing in June to prepare for this.

Ms. Chantal Bernier: While waiting for the act to come into force, we have started building our capacity to respond to the investigations we will have to do under the act.

The commissioner just referred to a day of training we are planning on June 20. For many months we have had a working group specifically on the implementation of the anti-spam legislation, so our entire office in its various functions is well coordinated on that. That working group has built an all-day training session to make sure that every part of our office is enabled and has the expertise and tools to be able to respond to complaints if and when they occur under the legislation.

[*Translation*]

The Chair: Thank you, but your time is up.

Mr. Andrews now has the floor for seven minutes.

[*English*]

Mr. Scott Andrews: Thank you very much. Welcome back for hour two.

I have one question. I'd like a little conversation around your upcoming workload with regard to the implementation of the perimeter security act.

What's your feeling on how big a piece of work that is going to be for your office? How many resource hours will you have to give to that piece of work? Is that one of the major pieces that you have coming up?

Ms. Jennifer Stoddart: Yes, I think it looms fairly large in our work expectations for this year, but because we don't know exactly what's coming out of this and exactly the timetable, because it's an ongoing process of exchanges between the Canadian government and the American government, it's a bit hard to predict exactly. But yes, national security issues are clearly, for all sorts of reasons, becoming even more important in our workload.

Mr. Scott Andrews: Has your office dedicated a lot of resource hours to it? Have you budgeted out what this piece of work is going to entail for the upcoming year?

Ms. Jennifer Stoddart: I don't believe we have, but perhaps the assistant commissioner would like to comment. It has taken a certain amount of time in the past.

Ms. Chantal Bernier: As the commissioner says, obviously analysts have spent a lot of time looking at that. The commissioner was talking about how it's looming large. In particular, she was referring earlier on to privacy impact assessments. The government has committed, as it has to do by Treasury Board guidelines, to submit to us privacy impact assessments on any initiative under the plan of action on a border security perimeter that would have repercussions on privacy. Clearly, that could be a significant source of work for us, and yes, that is part of our analysis as to how we will absorb that. But we will indeed have to address that challenge.

Mr. Scott Andrews: Will that piece of work have any impact on any other government departments that deal with national security and border security? Will you be relying on some other departments to provide you with information? Is there going to be a financial impact on other agencies as you go through this process?

Ms. Chantal Bernier: The way it works is that the department that is developing a measure has to develop a privacy impact assessment. They would have to do that; that is the workload for them. They submit the privacy impact assessment for our review and we make recommendations on integrating privacy protection to the measure; that is the workload for us. So, yes, clearly there will be workload on every side.

Mr. Scott Andrews: What is the timeframe on this piece?

● (1230)

Ms. Chantal Bernier: There are different points. As you know, we are coming to one of the first timelines, which is the production of joint privacy principles by the end of May. Then there are measures throughout the action plan on a longer timeline, and those will eventually have to produce privacy impact assessments.

Mr. Scott Andrews: Are you monitoring the privacy laws and applications on the other side of the border on this particular file as well? Are they doing the same thing? Could you elaborate on any concerns you might have on that aspect?

Ms. Chantal Bernier: We are working with the Americans right now to develop...not we, not our office, but the Government of Canada is working on the development of these joint principles, and we are regularly kept informed by the public servants in the Government of Canada who are working on this. We're given very broad development reports, and we will eventually see the principles and we will comment.

In relation to what is going on south of the border, obviously we read, we follow, we analyze.

Mr. Scott Andrews: Are there any areas of concern there that we should be aware of?

Ms. Chantal Bernier: Well, they're a sovereign country, of course, and we keep informed about their work in the sense of a context for ours.

Mr. Scott Andrews: Thank you.

That's all I have.

[*Translation*]

The Chair: Thank you.

Mr. Calkins, you may go ahead. You have seven minutes.

[*English*]

Mr. Blaine Calkins (Wetaskiwin, CPC): Thank you, Mr. Chair.

Thank you, Ms. Stoddart, for being here today. I appreciate the opportunity to ask you some questions. I have a number of questions that don't relate to what we're talking about this hour, but from the previous hour as well. I'll probably be jumping around a little.

I wanted to ask you about the cash on the domestic flights that CATSA was reporting to other law enforcement agencies or keeping information on. When I went through the report, I saw it was quite disturbing. It seemed as if over 50% of the information in the incident reports they were keeping was beyond their mandate.

I travel. I fly internationally several times a year and domestically every week, it seems. I have never been asked by any CATSA security screener if I have any cash, if I have anything at all. They sometimes look through the bags. Sometimes they just look through the scanner. Sometimes they'll ask me for permission to look inside the bag. I don't see anybody recording anything. So I'd like to know, when my bag goes through a screening device and it takes a picture or whatever, do they keep that? How is it that they find out that somebody is even carrying a large portion of cash? If my wallet goes through, all they see is my wallet. I can see the screen too.

A voice: It's pretty skinny.

Mr. Blaine Calkins: Yes, things are a little tight. But the reality is, I'm quite dumbfounded as to how they would even get that information in the first place, because the question is never asked. It would seem to me that even the collection of information...I don't know how they would possibly do it.

Could you enlighten this committee on how that happens?

Ms. Jennifer Stoddart: I think they can see quite a bit. My understanding is that they don't keep the images of the screening or the body scanners. If you look at their screens as your bags go through, that is perhaps how they look at it. You can then be subject to a secondary search if they see something suspicious. You will remember that when you enter and leave Canada, there's a declaration, "Are you carrying more than $10,000?"

Mr. Blaine Calkins: That's international, and that's fine. I understand it, and there are laws. It's an appropriate question to ask and it's an appropriate thing to check for. But domestically there is no law, and I think this is why the concern came up. I was a little shocked, because I go through there twice a week, 30 weeks a year, flying back and forth to Ottawa, notwithstanding other trips I may take in Canada.

Ms. Jennifer Stoddart: But you're not carrying enough cash.

Mr. Blaine Calkins: Whether I'm carrying cash or not, I'm not even asked the question. I would guess if I'm not being asked the question...why would they even be looking for it in the first place?

Ms. Jennifer Stoddart: My understanding is, and perhaps Commissioner Bernier, who worked more closely with the audit than I did.... They are looking at everything; they have to look at everything to understand that you are not carrying on yourself or in your baggage anything that could be a danger to Canadian aviation safety and so on.

In the course of doing that, they discover all kinds of things. It's amazing—some of these come up in the media—what people try to carry onto an airplane. One of the things that came up a lot was large amounts of cash, presumably under $10,000, because over $10,000 you have to declare it. Trying to be helpful, I think, the employees then would report this, but our job is to point out the potential problems with overreporting. If every agency goes a bit beyond its mandate to try to be helpful to something else, then they're not really following the law that Parliament has voted.

● (1235)

Mr. Blaine Calkins: The real issue is...I mean, I can see where a law enforcement agency—

Ms. Jennifer Stoddart: I don't know details about how they do it, but that's what we found.

Mr. Blaine Calkins: That's interesting. I can see where the information could be useful to a law enforcement agency, for example, if it is keeping surveillance on a person who has large sums of cash. Who is to say that the individual may have just sold a property or some large-value asset and is just taking the cash? There can be legitimate and illegitimate reasons for carrying large sums of cash. If the question is never asked, how would they even know, other than going through...? It just seems to me to be quite....

I thank you for bringing that up. I will be sure not to have more than a twenty on me when I go through security.

I'm going to refer to my personal life before I was a member of Parliament. You talked about the educational component of making people aware. I taught computer systems technology at Red Deer College. I am a graduate of computer systems technology. I am a little bit dated now because I have been here for a number of years and technology is advancing at a rapid pace. I'm just wondering, when we went through the accreditation process of having our diploma, we went through ASET, the Association of Science and Engineering Technology Professionals of Alberta. They would give us accreditation for our diploma so that graduates leaving that college would be recognized. It was a recognizable accreditation process.

Does your office ever get involved in making sure that anybody who has these accreditations actually has the wherewithal and knowledge they need? Do you make sure that somebody who graduates with a piece of paper has the knowledge? There is no official society out there for computer professionals. It's all voluntary. Is there anything that your office is doing to make sure those folks who are graduating, supposedly with the knowledge to maintain information systems and databases that would have all of this information, are actually trained to the level or standard that would satisfy most Canadians enough to know that whether they work in the public service or private sector, they are fully functional in the legislative requirements for the duties they would be doing? It seems to me that would be a logical place for an intervention.

Ms. Jennifer Stoddart: No, we don't, is the short answer, largely because education and training are the province of the provincial commissioners. They may be doing something.

Where it came up indirectly—and again, I'm not trained in this area, as you are—was in our Staples audit. We were amazed. This was the third intervention with Staples. This was the third time we heard there was a problem with Staples not being able to wipe the devices clean. I had understood from my IT people that, yes, devices can be wiped clean without destroying the hard drive or whatever are the essential parts that make it function. In the course of the audit, Staples—and this is what I understand from the people who did the audit—continued to say that it was not possible to do this.

This makes one wonder about the issue you are bringing up regarding the qualifications or ability of people who are in charge of processes like that. It comes up indirectly, because if businesses and the government are getting bad advice, we wonder how well the people are trained.

[*Translation*]

The Chair: Mr. Calkins, unfortunately you are out of time. You had seven minutes and forty seconds.

We will now start our five-minute round.

Mr. Angus, you have the floor.

[*English*]

Mr. Charlie Angus: Since my colleague Mr. Calkins was surprised that his seven minutes were up, I will follow up on one of his questions, which he might have wanted to follow up on in my five minutes. It concerns the issue of large amounts of cash.

I find this very interesting. Someone may carry a large amount of cash on a plane once. Perhaps the person just sold a house. Normally when you sell a house it is done through a bank. If someone carries large amounts of cash on two or three flights, that would seem to me to be a very large red flag, not that people pay attention to all of these flags, because they are drowning in data. As the Privacy Commissioner, when you are doing the audit, how do you decide what is an appropriate red flag to pass on and what is an inappropriate red flag?

● (1240)

Ms. Jennifer Stoddart: At this point, I have told you most of what I understand about the audit. Chantal Bernier, who supervised this audit, could perhaps complete my answers for you.

Ms. Chantal Bernier: The main point is that this information was collected outside the legislative authority of CATSA. There is absolutely no legal requirement to take it. It is not illegal to carry this amount of cash domestically. We were told that the reason they did that was almost for convenience. Because they needed to keep an eye on international flights in relation to carrying large amounts of cash, they did it for all flights. Hence, they gathered more information than they were allowed to. They easily conceded that they would stop that practice to be in compliance with the Privacy Act.

Mr. Charlie Angus: Part of it is that it's so easy to gather information, so easy to share information, and there are certainly concerns that you raise about integrating privacy into public safety initiatives. You have a pretty powerful statement that a new generation of mobile devices, remote sensors, high-resolution cameras, and analytic software have revolutionized surveillance practices and greatly facilitated the global collection, processing, and sharing of data. This unchecked accumulation could have negative effects on citizens and could have consequences by constraining people's fundamental right to go about their business in anonymity and freedom from state monitoring.

It's so easy to gather all this data under so many different strands. We have international police agreements and services, and they share data, and they have a reason to share data. Again, we deal with people crossing the border. Do they get stopped? There's a red flag that shouldn't be there. There's no legitimate reason for an authority to have that red flag, but they get stopped, and they can be greatly harassed.

How can you audit this kind of information, this kind of sharing, since it is so easy to do?

Ms. Jennifer Stoddart: That was, honourable member, in fact the very subject of an audit about what we did in maybe 2004-05, the sharing of information on border situations. We went to a large number of localities in Canada and just observed and looked at how the information was being recorded, and so on, and we made a lot of recommendations. We were shocked that sometimes things were kind of phoned across the bridge—"X is coming over, take a good look", or something like that. I believe this has improved, because we followed up on that audit and the implementation.

More than that, your question, honourable member, speaks to the importance of updating Canada's privacy legislation, which is the authority that the government has to deal with personal information and the authority that I have to look into its information handling practices. In previous sessions of Parliament I brought the issue of reforming the Privacy Act, which hasn't been looked at for 30 years, or hasn't been changed in 30 years, to this committee. The committee made a number of recommendations. I believe there were some 12 recommendations. Not only do we have to look at PIPEDA, but I think we should also look at the Privacy Act.

Mr. Charlie Angus: You're talking about the specific information that is shared. It's shared with the police services, the Insurance Bureau of Canada, and also with Interpol and American law enforcement. There were 200 million times when it was accessed through 40,000 access points in 2009. You say that a third do not have standards for ensuring protection. Are we talking about over 13,000 access points in Canada or is that internationally?

Ms. Jennifer Stoddart: A third of all those who have access privileges to the CPIC system have not defined within that organization or institution who it is exactly that designated the individuals, so it becomes impossible to track who in an organization has accessed something without justification. As you know from reading media reports, every so often somebody in a police force accesses a database where he or she has no business.

● (1245)

[*Translation*]

The Chair: Unfortunately, I have to stop you there.

Ms. Davidson now has five minutes.

[*English*]

Mrs. Patricia Davidson (Sarnia—Lambton, CPC): Thank you, Mr. Chair, and thanks very much for being here, Commissioner and Ms. Bernier. It's great to have you back again. Certainly, I don't think the issue gets any easier, that's for sure. I think it becomes much more difficult as we venture further into the electronic age every year.

I was interested in the public education portion you were talking about, and I just want to ask a couple of questions about it. I think you had indicated that from grades 7 to 12 you were already involved with education, and that this year you were moving it to grades 4 to 6. Also, this year you were introducing more information for small business.

Can you tell me how you disseminate that information? You talked about curriculum, but is that something that is written into the provincial curriculums in all of the provinces? I realize that it's up to the provinces to decide what goes into the curriculum, at least in Ontario, and I'm assuming it is in the other provinces. I know, not from this issue but from other issues, that it's very difficult to get something added to the curriculum.

Is it in all provinces, or do you know that?

Ms. Jennifer Stoddart: I don't know that. As you say, honourable member, this is a provincial matter. We're always very careful to stay within our own jurisdiction, unless we are invited to do something. What we have concentrated on doing is making the tools and information available on either our website or through things we can distribute when they are requested.

There is an agency, the Media Awareness Network, I believe, that works with school boards across Canada. If they request information, we can give it to them through this Media Awareness Network. It is just an additional resource for teachers, without formally going through the channels.

We also have, in our contributions program, $500,000 a year we can distribute to non-profit organizations. Just yesterday I attended the launch of materials for grades 6 to 9 in Quebec, where an organization had developed a very interesting teacher's guide and guide for students that it is going to distribute. It's talking with contacts in the rest of Canada, and it could possibly be translated and used for classrooms.

We do things in a more informal way.

Mrs. Patricia Davidson: What about small business? How do you reach that group?

Ms. Jennifer Stoddart: For small business we have an online tool already on our website. We go through the organizations that are involved with small business—

Mrs. Patricia Davidson: Do you mean the chambers of commerce and those types of things?

Ms. Jennifer Stoddart: Yes, they are specific organizations that reflect small business. We're particularly talking with the chambers of commerce now to organize activities for the coming fiscal year.

Mrs. Patricia Davidson: One of you indicated that you were looking at a mobile privacy app being developed.

Ms. Jennifer Stoddart: Yes.

Mrs. Patricia Davidson: Can you comment any more on that? What is the timeframe, or what might the parameters be, or are you that far on yet?

● (1250)

Ms. Jennifer Stoddart: No, I can't. I have someone here who could probably talk to you more about the mobile app. I don't know more about the details, but we're bringing it out.

I can tell you, though, related to that and related to the younger segment of the population, that we're developing a graphic novel on privacy, because young people like to read graphic novels, it seems. This is supposed to be launched sometime in June. I don't know what it's going to look like or what it's about. The theme is “protect your privacy”. It's trying to reach this audience in a way that speaks to them.

Mrs. Patricia Davidson: That sounds interesting and timely in the age we are in today.

Do I still have some time?

The Chair: You have 30 seconds.

Mrs. Patricia Davidson: Quickly, going back to what Mr. Mayes had asked about, if somebody trying to cross the border is incorrectly profiled, is there an option for the individual to report that through your office? How does that work? I think you indicated, too, that audits could be based on concerns being expressed. What is the individual's option in an instance like that?

Ms. Jennifer Stoddart: They can make a complaint. If they're flying, there is the office of redress administration. If somebody tells them that they are on a no-fly list, they can go to that.

Maybe Chantal, who looks at national security questions, can complete this.

Ms. Chantal Bernier: First of all, I would again talk about our website. We have a checking-in page that lists all the redress mechanisms when you travel, whichever way you travel, for occurrences such as, for example, the use of inaccurate information. In fact, we would be happy to bring you copies the next time we appear, but it is available on our website.

In addition to that, of course, people can make a complaint to our office, and we would then investigate.

[*Translation*]

The Chair: Thank you, but your time is up.

Ms. Borg, please go ahead for five minutes.

Ms. Charmaine Borg: Okay, thank you.

I know we have pretty well covered the topic, but there is something specific I want to ask you about. The other day, I read an article that said a survey had found that many people have trouble understanding the privacy policies of certain companies, such as Google and Safari.

Is that a concern for you? Are you doing any public education around that?

Ms. Jennifer Stoddart: The fact that privacy policies are written by lawyers who are not even Canadian lawyers and by courts that are not Canadian courts has always been a problem. It's a problem everywhere. For the most part, these policies are written with U.S. legal challenges in mind. That does nothing to help consumers in Canada or elsewhere. This is a frequent topic of discussion for privacy commissioners.

That being said, what tangible measures can we take? When a complaint is made, we tell the company it must clarify its privacy policy. Sometimes, companies say one thing and do another. Following up can definitely be a challenge. We devote a large chunk of our efforts to investigations, which often take months. Discussions with the companies are ongoing. We tell them they must clarify their policies because they have an obligation to explain to people what they do. So far, they have always complied more or less.

Ms. Charmaine Borg: There is still a long ways to go.

Ms. Jennifer Stoddart: Absolutely. These policies change all the time. The companies, themselves, change daily. Our most recent series of questions had to do with Google's new privacy policy. At the international level, the French data protection authority is asking the questions on behalf of all the data protection authorities.

Ms. Charmaine Borg: Thank you.

In your report, you also say that you often attend international conferences to obtain information. How does Canada measure up against other countries in terms of respecting privacy? Do you study that? Is that something these conferences help you determine?

Ms. Jennifer Stoddart: Yes, we often compare ourselves with others, because we are perpetually trying to improve when it comes to our performance and the protection of personal information. Canada has ranked better in the past than it does now. But given all the provinces and territories that have their own authorities, Canada has a fairly good reputation around the world. Canada is recognized as a country concerned with protecting the personal information of its citizens.

However, as I said, the legislation has not changed. PIPEDA has really not been amended since 1999. Thirteen years is a long time by today's standards. Public sector legislation has not been changed in 30 years. We still don't have any anti-spam legislation in force or any legislation on holes in security systems. Canada is already lagging behind, as I see it.

● (1255)

Ms. Charmaine Borg: How much time do I have left, Mr. Chair?

The Chair: One minute.

Ms. Charmaine Borg: The chair of the committee has already submitted a motion on this. We would like you to appear before the committee to discuss your concerns regarding the Canada-U.S. perimeter security action plan. Do you think the committee should look into that matter further?

Ms. Jennifer Stoddart: Yes, and I commend you on that initiative. I might recommend, however, that you wait until the next agreement on joint privacy protection principles is released so there is more content to study and discuss. As it stands, only the intention has been announced; you may want to wait until things are further along.

Ms. Charmaine Borg: Thank you.

The Chair: Just to clarify, is May 30 when we expect to receive those details?

Ms. Jennifer Stoddart: I believe so, yes.

The Chair: The last five minutes of our meeting go to Mr. Carmichael.

[*English*]

Mr. John Carmichael (Don Valley West, CPC): Thank you, Chair.

I'm glad to have the opportunity to address you, Commissioner, and your colleagues and I thank you for being here today.

As I've listened to your testimony and read the reports, I have to admit I marvel at the scope of your mandate. It's a big job and I commend you on the work you do. I think we're all thankful to have you in the role of carrying out the tasks at hand.

You've spoken today after eight years in your job and the changes you've witnessed, certainly in technology, which affects your role every day just as it affects our lives. We see it in the Internet and all the different spots. My colleagues opposite like to reference Bill C-30, a bill that's coming before this House and one that has raised intense concern on their side.

You mentioned that you have some concerns with that legislation and, I presume, with its predecessor legislation as well, going back to the previous Liberal government. I'm sure you'll be attending committee and will bring your thoughts forward. I look forward to that because I think you'll bring productive and beneficial input into that debate; that's something that I hope you will do.

As an aside, or as an extension of that, in the report on plans and priorities, one of the concerns I had was how you manage the change, day to day, in your organization. I notice that you mitigate some of the risk by implementing your change management strategy or talent management program. Is it enough to keep pace?

Additionally, because this is probably the last question you're going to hear today, as you think about the change management strategy, are you able to do enough to keep pace with the change that's coming at you? In addition, in the short and medium term, what major issues do you see facing your office, and again, coping with those within your department?

Ms. Jennifer Stoddart: Thank you for those questions.

In relation to change management, I would say we don't have a choice. We may not be changing fast enough to follow the issues. I know our staff often finds the rate of change that we have to maintain very difficult. In my opinion, either we change or we become largely irrelevant to the privacy problems of Canadians. That's the world in which we live and we have to deal with it.

For the future, increasingly in the online world, the mobile world, the implications of things like geospatial technology and biometrics continue to be in the forefront of our thinking. We rely on our four priorities to guide us. Genetic technology has huge implications for privacy. We talk about it for policing, but there's also the private sector; there is commercial business in genetic testing. There are issues around identity management. Identity theft is a huge online criminal activity. We haven't mentioned public safety and the use of drones. This will be a whole new era of public safety issues. As the web itself changes and then links with other technologies into a total technological environment, it will be a challenge for us to figure out the limits of this total surveillance capability.

● (1300)

[*Translation*]

The Chair: I have to stop you there, because we need to put the question to a vote. I will read it in English.

[*English*]

JUSTICE

Offices of the Information and Privacy Commissioners of Canada

Vote 45—Office of the Privacy Commissioner of Canada—Operating expenditures.....$22,131,000

(Vote 45 agreed to)

[*Translation*]

The Chair: Mr. Nadeau, Ms. Stoddart and Ms. Bernier, thank you for being here today. We hope to see you again very soon.

Meeting 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