



House of Commons  
CANADA

# **Standing Committee on Access to Information, Privacy and Ethics**

---

ETHI • NUMBER 020 • 2nd SESSION • 40th PARLIAMENT

---

**EVIDENCE**

**Monday, May 11, 2009**

—  
**Chair**

**Mr. Paul Szabo**

Also available on the Parliament of Canada Web Site at the following address:

**<http://www.parl.gc.ca>**

## Standing Committee on Access to Information, Privacy and Ethics

Monday, May 11, 2009

•(1535)

[English]

**The Chair (Mr. Paul Szabo (Mississauga South, Lib.)):** Order.

This is the 20th meeting of the Standing Committee on Access to Information, Privacy and Ethics. Our order of the day, pursuant to Standing Order 108(2), is our study on Privacy Act reform, and more specifically the quick fixes proposed in a report from the Privacy Commissioner.

Our witness today, after having a number of witnesses on the subject matter, is in fact the Privacy Commissioner, Ms. Jennifer Stoddart. She has with her the assistant privacy commissioner, Chantal Bernier, and acting senior counsel, Hedy Kirkby.

Welcome to all of you.

We've had an interesting journey with our witnesses and with our discussions with you in the past. I understand that you have some opening remarks for us with regard to what we heard. The committee has prepared a draft report, in camera, to encapsulate some of the witnesses' views as well as to get a preliminary indication of the committee's views. Now that we're here, full circle, back to the commission itself, we're very interested to hear your reaction, if any, to any of the matters raised by some of the witnesses or even by the members' questioning, to assist us in finalizing our report.

With that, I will turn the floor over to you, Madam Commissioner.

**Ms. Jennifer Stoddart (Privacy Commissioner of Canada):** Thank you very much, Mr. Chairman and distinguished members. It's a pleasure to be back here to conclude a journey that we've undertaken together over at least a year now. It's a year and a half that we've been talking about it.

My remarks today are going to highlight some of the important concerns, some of the reasons why I would encourage you to move forward to make recommendations for significant changes to the act.

We have enshrined in this latest document.... You'll remember that about a year ago, I guess in April, the first document we gave to you had eight recommendations, then the following month it went to ten, and because of witnesses and debates it's now at twelve significant things that we believe should be changed but that should not, we think, cause too much basic overturning of the structures of the act.

I'll begin by reminding us all that the Supreme Court of Canada, which is called to interpret our privacy legislation, has repeatedly affirmed the central importance of the informational relationship between the Canadian state and its citizens.

I had the pleasure of being at a training day for the government access to information and privacy community here in Ottawa last week, and Madam Justice came and gave a luncheon address herself and reaffirmed the importance of the work that the people in the ATIP community do and the importance of enshrining privacy.

The Privacy Act that you're looking at today has been accorded quasi-constitutional status because of the fundamental values it's intended to protect. However, as you have seen over the last year and a half, the act remains woefully inadequate to protect such fundamental rights in the face of new technologies, new ways of offering services, new imperatives, and new conceptions about privacy.

[Translation]

While other quasi-constitutional laws such as the Canadian Human Rights Act and the Official Languages Act have been progressively modernized to enshrine fundamental and contemporary Canadian values into law, the Privacy Act has remained virtually unchanged ever since it came into effect in 1983.

In the quarter century since, we have witnessed unprecedented growth...

[English]

**The Chair:** We have a problem with the translation from French to English. We're getting a static buzz.

We're going to have to suspend for a moment until the technician can deal with the problem.

•

\_\_\_\_\_ (Pause) \_\_\_\_\_

•

•(1540)

**The Chair:** Okay, we're going to resume the meeting.

Colleagues, a technician is on the way to help us deal with the problem of the translation of French to English. The commissioner can proceed, delivering in English. The French translation does work, and everyone will be able to hear the presentation in their language, either directly from channel one or from channel two. When we finish the presentation, unless the technician has resolved the problem, we'll have to stop again because of the questions and answers.

We'll let the commissioner finish her presentation, and then we'll see where we are.

**Ms. Jennifer Stoddart:** Okay. Mr. Chairman, I could repeat the question in the other language and repeat my answer in both languages, if that would help.

**The Chair:** Well, we'll see where we are when we get there. How's that?

**Ms. Jennifer Stoddart:** Okay. I'm very sorry. I will continue in English.

Barring a full revision of the Privacy Act, I've previously proposed that the government consider what we call quick fixes—this is a bit of a nickname, I guess—that might help address some of the more substantial shortcomings of the act. However, my view remains that a fully modernized Privacy Act would reinforce the pivotal importance of privacy rights and ensure that government institutions remain accountable and transparent with respect to the handling of personal information, and that my office can fulfill its mandate.

I'd like to go on and talk about the gap that's more and more inexplicable between our standards for public sector privacy and private sector privacy. I'm not suggesting, and I've not suggested over the time you have looked at this act, that the modernized Privacy Act should mirror PIPEDA in every respect. However, I do think it makes sense in this year of 2009 to align the Privacy Act with certain elements of PIPEDA. Expanding the definition of personal information to include non-recorded information, giving my office a clear public education mandate, and requiring ongoing five-year parliamentary reviews are examples of changes that would allow more uniform protection of privacy rights.

The proposal to broaden the grounds for an application for a court review is also meant to provide uniformity with respect to privacy rights. I should add that there's absolutely no discrepancy, in my mind, between providing complainants with the opportunity to apply for a court hearing following an investigation and providing me with a limited and specified discretion to refuse to entertain certain complaints.

Indeed, the Minister of Industry has recently proposed how I might exercise such discretion. Under Bill C-27, which creates a new electronic commerce protection act and amends PIPEDA, among other acts—it's an act introduced about three weeks ago—I would have the discretion to decline to investigate complaints or to discontinue complaints made under PIPEDA in certain specified circumstances. I could, for example, decline to investigate where there is a more appropriate alternative review procedure, more suited to deal with the complaint. As well, I would have discretion to discontinue a complaint in certain limited circumstances—for example, where the matter of a complaint has already been

investigated by my office. Bill C-27 would still allow individuals to apply for a court review, even if my investigation has been discontinued, therefore protecting an individual citizen's right to recourse to the Federal Court. If this has been adopted in Bill C-27, I respectfully put to you there's no reason the same approach could not be adopted under a revised Privacy Act.

I've also asked that my office be provided with greater discretion to report publicly on the privacy management practices of government institutions. This recommendation is intended to allow my office to put information regarding audits and specific investigations on our website on a timely basis and as events occur.

As I mentioned a year ago, security safeguards under the Privacy Act also lag behind those in PIPEDA, and mandatory breach notification should be considered for the Privacy Act, as it is being considered for PIPEDA. There's no reason to deny Canadians a certain level of consistency with respect to their privacy rights, regardless of the organization or institution in question. Indeed, the principles of accountability and transparency beg a higher degree of protection for personal information in the hands of the government, especially considering the position of trust in which citizens stand vis-à-vis the overwhelming machinery of the state.

You have heard from some of the witnesses who have come before you in the last year that we don't need modernization of the Privacy Act because we have policies on that. I'd like to address that particular point.

Several of our proposed reforms of the Privacy Act include the necessity of enshrining into law current government policies related to privacy. I commend the Treasury Board Secretariat for putting into place a policy on privacy impact assessments, for providing guidance to departments on information sharing with foreign states and the outsourcing of personal data processing, and for improving reporting requirements of government departments under section 72 of the Privacy Act. Nevertheless, such practices need to be circumscribed by law as a matter of ensuring the government remains accountable and transparent with respect to its personal information handling practices.

● (1545)

Privacy audits, reviews, and investigations carried out by my office have unfortunately shown that institutions are not consistently meeting their commitments under government policies and that government standards provide little assurance or information to Canadians, or even to parliamentarians, seeking to understand the privacy implications of government services and programs.

Privacy impact assessments are instrumental in addressing privacy risks associated with government programs. For example, my office worked with the Canada Border Services Agency when the enhanced driver's licence was being piloted in British Columbia. As a result of concerns we raised about the custody and control of the information on Canadians travelling to the United States, the agency agreed to relocate the database containing personal information on travellers from the U.S. to Canada. We would see more of these successes if the requirement for privacy impact assessments were enshrined in law so that Canadians and parliamentarians alike could have an opportunity to voice concerns and receive assurances that privacy issues were being addressed.

The truth is that it is far easier to ignore a policy than a legislative requirement. Indeed, some departments are still collecting excessive personal information, even though Treasury Board policy includes a necessity requirement. In a recent audit of Elections Canada, for example, we found that it was receiving personal information on young people under the voting age that was clearly not needed for a voters' list.

Parliamentarians need to have better information about how federal departments and agencies are doing managing the personal information they have from each and every one of us. Leaving it to the vagaries of policy and the good will of public servants is simply not good enough.

I'd like to just remind this committee of some of the recent events that suggest that we do, in fact, need stronger privacy protections.

The lessons of the past few years teach us that stronger privacy protections are needed if privacy is to have any meaning at all in the face of contemporary challenges. A recent EKOS poll commissioned by my office showed that 60% of Canadians feel that their information is less protected than it was ten years ago, 71% of Canadians see the issue of having stronger privacy laws as a matter of high importance, and only about one in seven Canadians is confident that Canadian law enforcement and national security authorities respect the laws that protect Canadians' privacy. These numbers, to my mind, speak volumes about the profound attachment that Canadians have to their privacy rights.

The recent events surrounding the O'Connor inquiry and the Iacobucci inquiry shed light on the information-sharing practices of national security and law enforcement agencies and highlight the need to hold government institutions to a higher standard of privacy protection, information handling, and data protection. Given the enormous trust accorded to the government and its institutions in relation to law enforcement and national security and their global implications, we need a more precise legal framework around information sharing in an international context.

In conclusion, in 1982 Canada took a leading role when it became one of the first countries to adopt stand-alone privacy legislation that applied to its government; however, the inevitable impetus of change has gotten the best of the Privacy Act. It no longer reflects our modern conception of privacy and is out of tune with the realities of contemporary government.

The committee's review of the act is certainly timely. It is joining an international trend in modernizing privacy legislation to meet the

realities of the 21st century. For example, the Australian Law Reform Commission has recognized that its own 20-year-old Privacy Act needs a host of refinements to help navigate the information superhighway. These refinements are currently under consideration by the Australian government.

Thank you very much for inviting me once again to this committee, Mr. Chairman, and I would be pleased to take any questions you may have.

• (1550)

**The Chair:** Thank you kindly.

I think I'd like to move straight on to the questions. We'll start with Mr. Wrzesnewskyj.

I would ask Mr. Siksay to please take the chair. I've just had a message and I have to take care of a matter. It will take a few minutes.

We can carry on with the questioning. I'll be back as soon as I can.

**The Vice-Chair (Mr. Bill Siksay (Burnaby—Douglas, NDP)):** Thank you, colleagues.

We'll go to Mr. Wrzesnewskyj for the first seven-minute round.

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

Welcome back, Commissioner.

Commissioner, is it correct that the RCMP produces the largest number of privacy complaints that your office receives per year?

• (1555)

**Ms. Jennifer Stoddart:** From memory, it is one of the targets of the greatest number of complaints.

**Mr. Borys Wrzesnewskyj:** Okay. Would you have an actual number of how many of those complaints are found to be valid?

**Ms. Jennifer Stoddart:** Yes, I believe I do.

I have to look at my last annual report. The Royal Canadian Mounted Police were ranked fourth in the number of complaints, with 52 complaints, of which three were well founded, two were well founded and resolved, nine were settled in the course of investigation, and one was resolved.

**Mr. Borys Wrzesnewskyj:** So nine were resolved in the course of investigation, three were resolved—

**Ms. Jennifer Stoddart:** Three were well founded. Two were well founded and then resolved after the finding of being well founded. They're just kind of nuances as to when either an agreement or a resolution was—

**Mr. Borys Wrzesnewskyj:** Now, if you take a look at those statistics, how do they compare with other government departments on the level of complaints that are well founded and resolved, etc.?

**Ms. Jennifer Stoddart:** I'd probably have to do a lot of quick mental arithmetic, at which I'm not too quick.

**Mr. Borys Wrzesnewskij:** Why don't we save that for after the meeting?

**Ms. Jennifer Stoddart:** Okay. We could provide that. I can say that consistently—and we understand—because of its activities, there are many complaints against the RCMP—

**Mr. Borys Wrzesnewskij:** I find an interesting correlation. The RCMP seems to garner among the highest number of complaints, while at the same time, when it comes to these recommendations, they seem to be the most resistant and, on some of them, almost intransigent in agreeing that some of these changes are necessary.

They tried to assuage the committee, I guess. They used the term—and it's in quotation marks, in fact—that it uses a “principled approach” when it comes to some of the concerns of sharing of information, especially with other governments and other law enforcement agencies around the world. It makes me somewhat curious that the very agency that seems to garner the largest amount of complaints doesn't seem to want to see these sorts of changes to protect a citizen's privacy, a quasi-constitutional right.

Let's take a look at the sharing of information with foreign governments. They said that, per year, the RCMP shares information on 4,000 requests with Interpol, and then 3,000 with other governments around the world. This creates a total of approximately 7,000.

On the 3,000 requests from around the world, do we have any idea, if we break them down, of which countries we're sharing information with? I would assume that most of the requests would come from the United States. Would countries that are not democratic and don't have the same sorts of human rights protections that we have—or even privacy protections—be among the list of the 3,000 requests per year?

**Ms. Jennifer Stoddart:** I would presume so, but not from direct or institutional knowledge. Perhaps it's more from the fact that the assistant commissioner and I appeared last Thursday at the public safety committee, along with the former counsel for the O'Connor inquiry, and we heard that this had been one of the highlights of the O'Connor inquiry: the sharing of Canadians' personal information abroad with countries that don't have satisfactory human rights records.

**Mr. Borys Wrzesnewskij:** We're in a very different world right now, too. We have biometrics, the ability to share genetic information, GPS, real-time video surveillance, and micro-surveillance in real time. We don't seem to have any protections in place, even here, when it comes to that sort of extremely personal information.

We also don't seem to have the safeguards in place in regard to how that information is shared, except for this statement by the RCMP. They don't agree with rules being put in place to make sure it's being safeguarded, and we're supposed to believe that they take a “principled approach”, so that should be good enough. Do you think that's good enough?

• (1600)

**Ms. Jennifer Stoddart:** No. I disagree with that approach, not only here, but in the public safety committee, where we appeared last week. This points to at least two of our recommendations. One is the necessary change from “recorded” simply to “information”. That is the standard in PIPEDA. That would allow the inclusion of privacy protections to such things as genetic data, GPS location, and so on, whether or not it was in a recorded form. Another recommendation that we think is not that difficult to implement and is necessary now is to have some kind of what we call in the jargon “privacy management framework” with standards.

What are the standards for the RCMP to share information abroad? On what conditions? How long is it going to keep the information? What is it going to do with the information? What are some tests for this information? We've called for a necessity test—I think this joins our recommendations to the other committee—and we need some kind of public oversight. The RCMP is the only body now that still does not have major oversight. And I think this may explain the lack of comprehension and the lack of empathy, I guess, with some of our suggestions, because presumably this would be material for oversight by an eventual oversight mechanism or committee.

**The Vice-Chair (Mr. Bill Siksay):** Thank you, Mr. Wrzesnewskij. That's your seven minutes.

[Translation]

Mrs. Thi Lac, you have the floor for seven minutes.

**Mrs. Ève-Mary Thāi Thi Lac (Saint-Hyacinthe—Bagot, BQ):** Good afternoon, Madam Commissioner.

I have three little questions. In your presentation, you said that there is no discrepancy between the fact that complainants... You refuse to investigate, because your discretionary power allows you to do so; complainants can go directly to Federal Court if your office refuses to investigate. But, for people requesting that recourse, it would not be without cost.

**Ms. Jennifer Stoddart:** Yes, that is a different question. There are costs when you go to Federal Court. There are costs, and the court is not available in all communities, only in some of Canada's largest cities. However, that does not come under the Privacy Act, so I have not commented on it.

**Mrs. Ève-Mary Thāi Thi Lac:** Are we not running the risk of creating a kind of two-tier system? You would refuse to deal with people's complaints and then they have to spend money to get information from the court that they would not have to pay for if you did the investigation.

**Ms. Jennifer Stoddart:** What is your question?

**Mrs. Ève-Mary Thāi Thi Lac:** Would that not be a form of justice denied for people who...

**Ms. Jennifer Stoddart:** There is that risk, but the problem at the moment, in my opinion, is the lack of discretionary power. Our office must focus on complaints where we can really have an impact, where we can do some good, and free ourselves of complaints that are not so much questions of personal information as other problems masquerading as complaints.

I feel that, in one sense, we are not providing very good service to people with real problems at the moment, because we are required to deal with a huge array of problems. I think that Canadians as a whole would be better served if we could take a little more selective approach and focus on new problems that we are seeking a solution to. However, because any government organization can make mistakes, in all fairness, we have said that, if we refuse to take up a complaint, we recommend that people go to Federal Court if they think a wrong has been done. They can seek justice there, but it should only be a minimum of cases, those where we see that nothing can be done and we are best out of it.

• (1605)

**Mrs. Ève-Mary Thāi Thi Lac:** You also said that audits and investigations carried out by your office have shown that institutions are not consistently meeting their commitments under government policies and current standards.

At the beginning of your presentation, you mentioned changes that could be made quickly. However, you did not list them. Could you provide a list of these quick-fix changes? Can you tell us how you propose to make institutions meet their commitments and your expectations?

**Ms. Jennifer Stoddart:** I think that the key is in recommendations 8 and 12 on the list. This would enhance the status of what, at the moment, are only Treasury Board directives. Within state apparatus, much more importance is given to the provisions of an act than to the contents of a directive that, at times, is inconsistently applied. For example, we do not always have privacy impact assessments. We are recommending that you include them in the amendments to the bill so that they receive the attention they deserve.

**Mrs. Ève-Mary Thāi Thi Lac:** Earlier, one of my colleagues asked you a question about requests from countries where human rights are not respected, countries with which we would perhaps prefer not to share information.

How do we ensure that this information is really protected from such requests? Would it be through your discretionary power? How do we detect these requests and how do we deal with them at the moment?

**Ms. Jennifer Stoddart:** We have to significantly reinforce the requirement in the current act for departments and agencies—we were talking about the RCMP just now—to be more careful and vigilant about putting things in writing. A matter of national security does not have to be made public. What is the information that we are going to share with such and such a country for such and such a purpose? What will be done with the information? We would have to make a comprehensive list of the countries and organizations with which we exchange personal information. Eventually, if the government establishes an oversight organization, that organization

could make sure that the RCMP complies with the understandings, the exchange lists, the agreements.

[English]

**The Vice-Chair (Mr. Bill Siksay):** Mr. Dreeshen, for seven minutes, and then hopefully we'll come back to my spot if Mr. Szabo is back in the room.

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

Ms. Stoddart, I want to welcome you back here to discuss privacy and ethics reforms. I personally thank you for your ongoing leadership in a time of increasing public concern for Canadians regarding privacy issues. You spoke of the new technology, the new ways of offering services, and the information superhighway. All of those things are important to us all.

As commissioner you've concluded that there could be some benefits if the Privacy Act and PIPEDA were more closely aligned. Other reforms seem to be inspired by provincial approaches to ATI and privacy legislation. These issues, whether it be the Privacy Act or PIPEDA, or provincial responsibilities versus federal responsibilities, should be reflected, I think, when we consider these Privacy Act reforms. Perhaps as you answer some of our questions you could keep those points in mind and reflect on them as well. I'd appreciate that.

Your first recommendation would create a legislative necessity test, which would require government institutions to demonstrate the need for the personal information they collect. Does section 4 of the Privacy Act not already include a necessity test for the collection of that personal information?

• (1610)

**Ms. Jennifer Stoddart:** I believe the current test is simply the consistent use once the information is gathered. I think it's very important for the Privacy Act to mirror not only PIPEDA but much provincial legislation, in that there's a test. You can't just collect anything and then say you'll collect anything. There's only a limit as long as it's used consistently.

There's an initial test: there has to be a reason for it, there has to be some kind of necessity. In the provinces, if you look at them generally, there's either necessity or law enforcement, which is a general...I won't say it's an exemption, but it's a recognition of the particular role of public security forces like the police, or legislation. There's specific legislation the legislature has addressed its mind to and said the government will collect information for this. You have none of these specifics in the current Privacy Act, and in PIPEDA there's information that a reasonable person would consider justified in the circumstances for the purposes. So I'm contrasting both the provincial and PIPEDA to the general laissez-faire approach of the Privacy Act.

**Mr. Earl Dreeshen:** Would policy change rather than a statutory change be more appropriate to ensure the flexibility the minister recommended last year?

**Ms. Jennifer Stoddart:** I'll come back to my remarks about policy. We think, having observed for over 25 years, if you look at the series of annual reports done by me and previous privacy commissioners, the things that are merely put in policy are often not taken seriously enough. Perhaps it didn't have the consequences, let's say, in 1987 that it does now, but we think this is the time to elevate them into legislation. There are also extensive exemptions in the Privacy Act. There are quite a few exemptions, so I think they would also apply to a necessity test.

**Mr. Earl Dreeshen:** The minister had talked about a potential conflict between recommendation number two and recommendation number six. On one hand, you're broadening the application for court review, while on the other you're giving yourself broader discretion to refuse or discontinue complaints. Going that route would create greater grounds for appeals to the courts. As guardians of the public purse, we are concerned about these two recommendations, which are not only at odds with each other, but if they're implemented they could place an undue burden on the courts and the costs associated with these sorts of appeals. I was just wondering if you could comment on that.

**Ms. Jennifer Stoddart:** Yes. Perhaps I could direct the committee to look at the history of my office's experience under PIPEDA, where we have slightly more powers to deal in a more summary fashion than we do under the Privacy Act, and the relationship between those powers and the number of complainants going to the Federal Court. There are very few. I think right now, in terms of active complainants in the Federal Court where we're not involved, from memory we might have maybe five or six. These are people who go on to Federal Court. In recent years—I hope I'm not being inaccurate—I think almost all of them have lost or withdrawn their cases; the court did not find their cases had merit. I don't think that is a huge burden on the public purse. Of these six cases, let's say there are perhaps three now where we're active. Most of them are people going on their own, so there would be no cost via my office.

**Mr. Earl Dreeshen:** Going back to what Mr. Wrzesnewskij said, you were talking about the RCMP and the number of complaints there. Of course, we look at the five main issues. I guess the five people had complaints that were well founded. Basically, you're saying your department doesn't consider over 90% of them to be well founded. I guess if you're looking at it from that point of view, would the RCMP be considering this as a majority of the complaints that come their way are not ones they would perhaps consider major?

**Ms. Jennifer Stoddart:** If I look at it as 52, I read only three are well founded, two are well founded and resolved, and all the others are resolved, settled, not well founded, or discontinued.

• (1615)

**Mr. Earl Dreeshen:** I guess I was just looking at whether it's all negative when you're trying to consider five out of 52. I'm not saying there aren't problems, but certainly sometimes it's perception in degree as to what some of the concerns might happen to be.

**Ms. Jennifer Stoddart:** Yes, but if I may say so, the possibility of going to Federal Court in our experience usually focuses both parties on seeking a settlement.

**Mr. Earl Dreeshen:** If I have enough time, I will just ask one more question. What do you think the cost implications would be of going to recommendation three, and which could not be achieved through policy change rather than a privacy impact assessment legislative scheme? I think you had spoken about that before.

**Ms. Jennifer Stoddart:** That's an interesting question, because under the directives there is supposed to be a privacy impact assessment for every program now. So theoretically the money is in the departments. So I don't see that a case has to be made.

Departments are supposed to follow directives to get any more money, because it's now in the act. What we've simply said is that somehow directives aren't followed, but the money should already be there to follow the directives. So I would think there would be no cost of implementing recommendation three.

**Mr. Earl Dreeshen:** And would it be the same for provincial agencies as well as federal agencies?

**Ms. Jennifer Stoddart:** This wouldn't affect provincial agencies; it would just be federal agencies. They're supposed to be doing this. I'm just making the point that they're not doing it; that's why I would like you to put it into law. But my understanding is that they've already been granted the resources to do this, because this is a directive they're supposed to be following.

**The Chair:** The PIAs would certainly be helpful to the legislators as well, to understand the impact of changes to policy.

Mr. Siksay, please. And thank you for sitting in.

**Mr. Bill Siksay:** Thank you, Chair.

Thank you for being here again, Commissioner, with your colleagues.

I note that you've added two new recommendations this visit. I have this vision of seeing a list of 14 down the road, and then maybe 16. I hope it doesn't come to that, because I hope we can make some progress in moving on these ones before us.

I wonder if you could say a bit more about the new recommendations 11 and 12. I think we heard about number 11 in the context of a duty to protect, and I wonder if you could say a bit more about that. Then I think on recommendation 12, witnesses phrased it to us in terms of the duty to notify. I just wondered if you could say a bit more about those two.

**Ms. Jennifer Stoddart:** Yes, both of them are cases of what I was discussing with the previous honourable member; that is, they are in fact policies. Obviously the Government of Canada has a security policy and Treasury Board has breach notification guidelines. Again, we don't hear much about problems with data being lost or misused in the public sector, but we know there are some problems. We know them often from the media. Occasionally we'll hear something from the government itself. But again, there's a kind of momentum, as I was describing to you about going to Federal Court. If you put this into a law and you say there are breach notification guidelines and that they have to inform the privacy minister when there's a breach notification, I am hoping this will mean that these issues will be taken more seriously and that there will be fewer stolen laptops with citizens' information found under bridges, as we reported a couple of years ago.

**Mr. Bill Siksay:** One of the other recommendations we heard was about order-making power for your office. I know it's not one that you've recognized, but I believe it's also something you're working on or are investigating further. Can you say a bit more about that?

**Ms. Jennifer Stoddart:** Ye. You will notice I haven't asked for order-making power, because that would not be a quick fix, to say the least. It would involve looking at the whole structure of my office. In fact, in the context of PIPEDA, I am commissioning work by some scholars to look at the things that weren't looked at when PIPEDA was brought in. Many people now say we should have order-making powers, and the Information Commissioner has asked for limited order-making powers. So I am commissioning a study that should be out this year. But again, that's not something that's already in a directive. If you look, we do most of these things already, or they've been suggested, for example, by the O'Connor inquiry, or they're not radically different.

**Mr. Bill Siksay:** So it's not a quick fix, but it's something that is worth further consideration?

**Ms. Jennifer Stoddart:** It certainly is, and we're looking at that, yes.

**Mr. Bill Siksay:** I wonder if you can take us through recommendation five again. Certainly I have had some questions about just what you were requesting there. Could you explain what your reporting powers are right now and how this would change as a result of this quick fix?

Right now you talk about having annual and special reporting provisions, but is this recommendation aimed at giving you the ability to report more often, for instance, and outside of that, and to be more like the Auditor General, who has the ability to report as often as necessary? Is that what you're talking about, and not having to wait until the end of the year? Could you just expand on exactly what you're looking for?

• (1620)

**Ms. Jennifer Stoddart:** It's exactly that kind of thing, to have specific reporting powers so we can keep up with the modern media.

Maybe Hedy Kirkby can explain the problems with the current Privacy Act.

**Ms. Hedy Kirkby (Legal Counsel, Office of the Privacy Commissioner of Canada):** I'll start by mentioning that under the private sector act, PIPEDA, there is a specific provision that enables

the commissioner at any time, at her discretion, to disclose information concerning the privacy management practices of private sector organizations. When there is a matter the commissioner wishes to bring to public attention, she may do so. In so doing, the name of the complainant is never identified, but the name of the organization is.

A similar type of provision would be welcome in the Privacy Act, because currently it has nothing whatsoever other than provisions that speak specifically to annual reports and special reports to Parliament. It's unclear at best, legally, what the ambit of the commissioner's power is to go public upon completion of an investigation, for example, in which she would identify the government institution by name.

**Mr. Bill Siksay:** Right now, there's the ability to do an annual report and special report. How are special reports defined? What would they look like under the current regime?

**Ms. Hedy Kirkby:** We did a special report recently for the audit of the exempt banks of the RCMP. I believe we also did it for the joint audit that was conducted with the Auditor General more recently. On those two occasions, these were important issues that we felt should be brought to the Canadian public in a timely way.

**Mr. Bill Siksay:** What would be different from a special report, in terms of what's being proposed now?

**Ms. Hedy Kirkby:** Those are large reports that have Parliament as their intended audience. They are presented to Parliament, as is an annual report. What is envisaged is that on a smaller, more periodic basis one could report in a more summary fashion on interesting developments and decisions made by our office.

**Mr. Bill Siksay:** Report to where or to whom?

**Ms. Hedy Kirkby:** It's to the Canadian public by putting information on our website. That's the way we do it currently for the private sector act. We simply put up a case summary.

**The Chair:** Thank you.

I'd like to pursue that. I know the members were a little concerned about it going around Parliament. Let's deal with the question about how we respect your responsibilities to report directly to Parliament before the public. Are we anonymizing or de-identifying persons? Are we giving information out that may be interpreted as maybe being too specific, or are these generic or general developments based on case consideration?

**Ms. Jennifer Stoddart:** The intention certainly is not to go behind Parliament. The intention is to try to tailor the language of the 1983 Privacy Act to the way with which the public is used to being communicated to in 2009-10. How do you get a message about the protection of personal information to Canadians, particularly the younger generations now, if your primary vehicle is, for example, an annual report? By the time it's done and so on, it's 18 months after things have happened.

We would like to have a more flexible approach. For example, we could report to Parliament at much closer intervals. We could and do put some anonymized information on the website. We could perhaps make public some of our audits, so that Canadians know what to expect and have more transparency about the government's handling of their personal information. If you look at what we do in PIPEDA, you'll see an example of how we would like to deal with the Privacy Act.

● (1625)

**The Chair:** Let's look at what the Auditor General does now. The Auditor General can report to Parliament as often as she wants, but the Auditor General also participates, as you do, in conferences, in speeches, in visitations, and in interviews, when asked, I assume.

Does what you're proposing go beyond what the Auditor General might do in terms of the safeguards she would have?

**Ms. Jennifer Stoddart:** No, we would never jeopardize the protection of personal information nor our relationship with Parliament.

If we could have the possibility of going to Parliament whenever we wanted to, if for example we had done some kind of audit that we thought you should know about, we could kind of turn it around a lot faster and lay it out before you specifically rather than waiting 18 months and saying it's a special report. It would have to be a very big audit to be a special report. So we need something in between.

**The Chair:** All right. That's fair enough.

We'll go to Ms. Simson, please.

**Mrs. Michelle Simson (Scarborough Southwest, Lib.):** Thank you, Mr. Chair, and thank you, Ms. Stoddart, for re-appearing before the committee. It's been an eye-opener.

I'd like to ask you about recommendation four, which is to provide your office with a clear public education mandate. That recommendation has been supported by a number of witnesses. However, it doesn't have the support of the Minister of Justice and his department. His position was that this power already is implied within the existing act.

I'm sort of looking at the wording. You want it clear, while he's talking about implied. What is it that you would like clarified in terms of making it a little sharper or crisper and having it enshrined in the legislation?

**Ms. Jennifer Stoddart:** That's interesting that you quote the Minister of Justice as saying that this power's already there, because in fact my office noted that the Minister of Justice used this recommendation as an example that some of the proposed changes we suggest may be possible. So I don't know. I think he appeared several times. That's more my reading of it.

**Mrs. Michelle Simson:** I was just looking at the summary we received. There were witnesses who supported your fixes and those who maybe objected or did not support your recommendation. It was strange.

**Ms. Jennifer Stoddart:** Yes, we come to slightly different conclusions, but I will answer your question.

The public education mandate is not specifically spelled out in the Privacy Act, again in contradistinction to PIPEDA, a much more modern law. As a consequence of that, I believe that we don't really have the resources for a public education campaign or public education activities in terms of informing Canadians about their privacy rights vis-à-vis the government.

We don't, for example, have specific allotted resources to do research on national security and privacy issues, as we do under PIPEDA, with its specific contributions program that was written right into the law. I distribute grants every year so that people can do research into the impact of PIPEDA on their privacy. I think that would be very useful in terms of developing public policy.

That's the difference. It would make a big difference in terms of what we can do with the broader public.

● (1630)

**Mrs. Michelle Simson:** That's great.

Mr. Siksay noted that you added two additional quick fixes. Are there any other immediate quick fixes you would recommend? Lately we've been reading a lot about Google Street View. There seems to be a huge concern about that particular program. Reading about it in the paper, it would appear that the concern of your office has a lot to do with the storing of the images.

When I read through your report, I really appreciated the fact that there is a great concern about the storage of information, which could impact the privacy of citizens. Would these quick fixes, if they were all adopted, cover off things like Street View, or is there something more specific we could be doing? It appears that there's a great deal of alarm on the part of the public, and this is also something you were taking extremely seriously, based on the media reports.

**Ms. Jennifer Stoddart:** These changes would not address the issue of Google Street View because Google Street View is covered by the other law, so we are applying that other law to it. It is, shall we say, a challenge for the moment. The challenge isn't so much the law as it is the relative novelty of the kind of collection of personal information that's suggested by Google Street View, but I understand you're going to have hearings and so on.

Let me say that there are other recommendations. Initially, we had a long paper of some 50 pages that we submitted to this committee, and we've since been trying to refine our suggestions.

I and the assistant commissioners would be extremely happy if you were to adopt these 12 recommendations. That would be a quick fix. More than that wouldn't be a quick fix, but a major reform. We're trying to be practical: we're trying to suggest things that are already in practice, things that are low in cost, and things that simply underscore existing Treasury Board directives.

Of course, if you want to go on, we can, but we would be very happy if you accepted these suggestions.

**Mrs. Michelle Simson:** Thank you.

With respect to recommendation eight, which is to strengthen the annual reporting requirements to cover a broader spectrum of privacy-related activities, can you outline the activities that broader spectrum would include and perhaps why you're recommending their inclusion? In other words, what are we missing that we should be including?

**Ms. Jennifer Stoddart:** Over the years we've found that reporting on Privacy Act compliance is either absent or perfunctory, so we would like to change this from a directive to a part of the Privacy Act.

We'd also like some stipulation as to what they would be reporting on. Examples might be privacy impact assessments, initiatives that might have an impact on personal information, or information-sharing agreements with other government departments and agencies, other provinces, or other jurisdictions in Canada. These are examples of data-matching or data-sharing.

All these things go on, and it's very hard to trace exactly how they're happening. The reporting is rather obscure or non-existent. This would make what's happening with their personal information more transparent for Parliament and for Canadians.

**Mrs. Michelle Simson:** This is my final question.

In earlier questioning, you made reference to the fact that the act is from 1982. I agree that major revisions are probably required, but you did touch on the fact that there are currently a number of exemptions under the act. Can you give me a few examples of the exemptions in the current act that we perhaps should have included in any new legislation?

•(1635)

**Ms. Jennifer Stoddart:** We haven't suggested changing the exemptions.

**Mrs. Michelle Simson:** I'm just curious to know what they are. I don't specifically know.

**Ms. Jennifer Stoddart:** I'll ask Hedy Kirkby to talk about the exemptions. There are a whole series of them.

**Ms. Hedy Kirkby:** The focus of the materials we've presented to the committee is more on the privacy protection side than it is on access to information, which is the corollary right to privacy. The Privacy Act contains both rights.

With respect to access to information, the only specific recommendation we made was that the right of access should be extended beyond the status quo, which is limited to persons present in Canada. That's becoming increasingly difficult to defend, given the international trends to make the right universal.

We don't go into the specific exemptions in any particular detail because, on the whole, the exemptions work quite well. The exemptions in the Privacy Act very closely mirror the exemptions you'll find in the Access to Information Act, and since that's the primary focus of the Access to Information Act, that's where you hear the Information Commissioner focusing their recommendations for change.

**The Chair:** We'll have to leave it there. Maybe we can come back to that.

Go ahead, Mrs. Block, please.

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

Welcome, Ms. Stoddart and colleagues.

I'm interested in going back to recommendation four and following up on Ms. Simson's questions. You stated that the public education mandate is not spelled out, and that if it were, quite possibly there would be an ability to allot certain resources towards public education. Could you describe to the committee what you intend by proposing a public education mandate, what components you would include in that public education mandate, and what the costs of such a program might be?

**Ms. Jennifer Stoddart:** First, honourable member, we haven't costed it because we're crossing our fingers that it will be recommended by this committee, and then, of course, we would cost it. If committee members wish, we could supply you with the amount of our public education budget for PIPEDA to give you an idea. Now, these are organizations across Canada, so it might not be exactly the same.

I mentioned funding research across the country in universities, small business, and citizens' organizations, and providing information to what in PIPEDA are called interested stakeholders. These are organizations that use PIPEDA and need help in its interpretation. If you translate that into the Privacy Act, these could be campaigns with national security organizations to clarify the problems they would have in applying the Privacy Act and to see how we could work better with them. It could be working with citizens who ask what their rights are now that our frontiers are becoming increasingly problematic in terms of privacy rights, or perhaps working with the Canada Border Services Agency.

All of this takes a certain amount of investment in media communications to get more up-to-date information brought out more quickly, and particularly to get young people interested in issues of privacy as they relate to government use of their personal information.

**Mrs. Kelly Block:** In the world where I come from, it would be interesting to consider that we would make the recommendation without knowing what the costs could be.

**Ms. Jennifer Stoddart:** If the committee asked us for the cost, we could certainly give you some information on that very soon.

**Mrs. Kelly Block:** When we speak to the fact of an education mandate, the power is already implied. Do you feel that you couldn't achieve the same benefit without a legislative change?

• (1640)

**Ms. Jennifer Stoddart:** My colleague the assistant commissioner thinks that perhaps the reason for the discrepancy in the notes is that it was a spokesperson from the ministry of justice who said the power was implied.

It's one of these difficult questions. You think you should be informing the public in a more timely, up-to-date, modern way, but your act doesn't specifically say it. Honestly, I'm a bit torn between what I should be doing and not straying beyond the bounds of my mandate. The fact is I don't have particular financing for it. I think I should inform Canadians of challenges with their personal information—for example, the RCMP exempt banks—but the audit took money, the special report to Parliament took money, and so on. That's an example.

It would be to enhance the kind of public education activities that I already do under PIPEDA, but on the side that involves the personal information that Canadians give to the federal government.

**Mrs. Kelly Block:** Thank you.

Do I have any more time?

**The Chair:** Yes, you do. You have two more minutes.

**Mrs. Kelly Block:** I would like to look at your fifth recommendation. It would provide greater discretion for the Office of the Privacy Commissioner of Canada to report publicly on the privacy management practices of government institutions. As I read it, I thought that too might be part of a public education mandate.

How frequently would you like to issue these reports?

**Ms. Jennifer Stoddart:** I think the example of the Auditor General is very useful.

My understanding is that she goes four times a year. That would certainly give us more immediacy than once a year, because it ends up being a year and a half after things have happened. In this day and age, and especially to an electronic generation, you lose credibility about the message if you're reporting on it a year and a half later. People are living their news instantaneously now, so I'm concerned about shortening the time span between when things are happening and when, to be faithful to my mandate, I inform the public about them.

**Mrs. Kelly Block:** What additional resources do you think you'd require to complete these reports? Are you already doing them? Do you already have sole responsibility?

**Ms. Jennifer Stoddart:** No, we don't. We've done two special reports to Parliament, both on the public sector. That's within my present mandate.

If we speeded up the reporting cycle, that would take additional resources. My office is very small, so when we're talking about additional resources we're talking about two or three people, things like that. We're not talking about large amounts of resources because we operate on a fairly small scale anyway.

**The Chair:** Thank you.

Monsieur Nadeau.

[*Translation*]

**Mr. Richard Nadeau (Gatineau, BQ):** Thank you, Mr. Chair.

Good afternoon, ladies.

Recommendation 11 reads as follows: "Introduce a provision for proper security safeguards requiring the protection of personal information". Does that mean that we do not have them at the moment?

**Ms. Jennifer Stoddart:** Actually, that is another of those curious circumstances. There is a Treasury Board directive on security and the protection of personal information. But in my experience and that of my predecessors, a Treasury Board directive does not seem to get the attention it requires from the department, certainly much less so than if were in an act. I do not wish to imply that there are no security safeguards. The government is presently developing a cyber security policy, and that is very important. I am very pleased that they are moving forward, but we are talking about day-to-day administrators of the act. I think that Parliament sends a much stronger message if it puts some minimum requirements into legislation, if it enshrines in legislation the basics of what needs to be done. We feel that these 12 recommendations make up those basics.

Subsequent interpretation and details can then be put into Treasury Board policies. However, since there has been no reform for a very long time, the basics are now to be found in the directives. A directive is just a directive, and the consequences are much less weighty than those in an act.

**Mr. Richard Nadeau:** Do you feel, as we do, that an act designed to correct the present situation would be perfectly appropriate and that the government should respond to the request for one?

• (1645)

**Ms. Jennifer Stoddart:** I do. At the moment, those provisions are in the Personal Information Protection and Electronic Documents Act that you passed in 1999. My colleague showed me the relevant paragraphs. I repeat: we have already tried these things in Canada. They are in the other act dealing with the private sector. We are saying that, if the government has legislation for the private sector, the least it can do is have the same standards for itself.

**Mr. Richard Nadeau:** That is what we call leading by example, right?

Recommendation 9 reads as follows: "Introduction of a provision requiring an ongoing five-year parliamentary review of the Privacy Act". In your opinion, would that review provide recommendations for updating the act, since society is changing at an astonishing rate in matters of personal information. Is that why you thought in terms of the five-year period?

**Ms. Jennifer Stoddart:** Exactly.

**Mr. Richard Nadeau:** Does that exist elsewhere? Are there models that you could tell the Government of Canada about, whoever developed them? Are you able to say that in this place, in that province, in the other country, there are examples and that we are a backward country in that respect? Do you have examples for us?

**Ms. Jennifer Stoddart:** We are not a backward country, but we are perhaps a little inconsistent. I repeat: in 1999, this very Parliament passed a bill that governs the private sector—this was the committee that studied it—and that requires that the legislation be reviewed every five years. Provincial legislation in Quebec also requires a review every five years. A number of other provinces—Alberta and British Columbia come to mind—have the same provision. It is quite common and we even have it in our own legislation governing the private sector.

**Mr. Richard Nadeau:** What would you recommend to the committee to move on quickest? I imagine you want us to move on the 12 recommendations. I agree with you.

**Ms. Jennifer Stoddart:** Yes, I would like you to move on the 12 recommendations.

**Mr. Richard Nadeau:** Do we really need the 12 recommendations or should some things be done on a priority basis?

**Ms. Jennifer Stoddart:** I feel that that is perhaps the committee's role. Of all the many changes that could be made, I chose these 12 basic recommendations. They are all to be found elsewhere, either in legislation or in a directive. I think that the choice is up to you.

**Mr. Richard Nadeau:** You are asking us to push for the 12 recommendations.

Thank you very much, Mr. Chair.

Thank you, Madam.

[*English*]

**The Chair:** Merci.

Mr. Tilson, please.

**Mr. David Tilson (Dufferin—Caledon, CPC):** Thank you, Mr. Chairman.

I'd like to return to the issue of education. I agree there's a need for education. I'm looking at your recommendation four: "While PIPEDA provides the OPC with a public education mandate, the Privacy Act does not do so explicitly." What does the Privacy Act do?

**Ms. Jennifer Stoddart:** It doesn't mention, as I remember, public education at all.

**Mr. David Tilson:** One of the problems I have from my perspective is that in my riding most members of the public know there's a Privacy Act and they know that people have the Privacy Act and they know there are laws, but they have no idea what the laws are. Really, they haven't a clue what the laws are. They think they can demand such-and-such information from the government. No, you can't, because there are privacy laws.

So I look at your recommendation and I see you're saying that you're going to talk about publishing a compendium of significant cases; you're going to have public advisories and education material;

you're going to try to satisfy the needs of professionals; and you're going to publish research. Is there anything for the general public that you're contemplating?

**Ms. Jennifer Stoddart:** What we find is that you have to take the general public, and because it's so different in terms of age of interest, it's fragmented. But certainly, yes, there would be things for the general public. In schools, for example, we make some information available now on PIPEDA, in conjunction with the provincial commissioners, in a discretionary fashion because this is a provincial jurisdiction.

Many of the privacy laws across Canada resemble each other. That's another kind of education we could do. We could do more public education for seniors in terms of the use of their social insurance number, and on issues of privacy in getting some of their pensions. These are programs....

We have regional outreach initiatives and we are now cooperating with our colleagues in the Maritimes and in the prairie provinces. We're doing this under PIPEDA because we have a specific mandate for it. Again, issues like electronic driver's licences, which are Privacy Act issues, also concern the commissioner in B.C. and the commissioner in Quebec; there again, we could undertake joint efforts, but we confine them to PIPEDA.

• (1650)

**Mr. David Tilson:** I think that's admirable. The concern I have is that we're now into a recession, and money is a problem. It's fine to have great ideas, but some of the things you're talking about are being done through the provinces, through PIPEDA. It's already being done.

I'm not concerned with your saying let's have something under the Privacy Act, but you have indicated you're not too sure what this is going to cost. I think that before this committee makes any report to Parliament, we should know specifically what your plans are with respect to education, and specifically what that's going to cost. All of those items I read off that you have listed in your recommendations—publish a compendium of significant cases, etc., and I won't repeat them—are excellent, but what's that going to cost? And what is it going to cost to do what the provinces are doing and what PIPEDA is doing because you would therefore expand your education practices to the general public? The committee needs to know that before it can make any recommendation whatsoever to Parliament.

**Ms. Jennifer Stoddart:** I understand the honourable member's concern about public money, about possible overlapping. I assure you that we would not overlap and repeat what the provinces are doing or what we do in PIPEDA. But may I remind you that we're in a bit of an unusual situation here. Usually, when draft legislation or issues for legislation go forward, they go forward from a government department that has done that kind of costing and is set up to do that kind of costing with Treasury Board. Here, we are looking at something that is a suggestion of an agent of Parliament who does not have the costing function of Treasury Board, although we could provide you with that information.

What I'm saying is, if you think the principle is a valid principle, I would urge you to include it and then leave to Treasury Board, in the second time, the possibility and the discretion to say whether or not the public purse at this time can move forward to allocate those resources. Don't shut the door on the principle, but simply leave it to Treasury Board and to the Treasury Board Secretariat to decide whether or not that particular item should be funded.

That would be my suggestion, honourable member.

**Mr. David Tilson:** Any time I've heard you come before this committee, you're continually talking about the backlog of your investigations. There's only so much money that's going to be allowed, even in these difficult times. The question really would be, if we provide for an expansion of cost for an education mandate, how would that take away from the other work you're doing, unless it's an add-on? Either way we have to know the figures, and if we don't know the figures, we still have to know whether it's going to take away from something.

Either way, it's a problem for this committee to make recommendations, in my opinion.

**Ms. Jennifer Stoddart:** I would suggest, honourable member, that this is a function of the Treasury Board Secretariat. I'm not here before you to ask for more money. I don't have any requests for more money. I'm here because I'm concerned about the principles in the Privacy Act that need to be updated. If you share my concerns, I would ask you to update the act.

There is a special parliamentary panel on which some of these members sit. These members can then discuss with me whether I have any needs. Treasury Board weighs in, and Treasury Board finally gives any credit. I'm not there yet. I'm here on the principles and I would put it to you that reforming the Privacy Act does not commit you to necessarily funding all the different provisions.

•(1655)

**Mr. David Tilson:** There's a cost to everything. I can generally agree on the issue of education, just from the simple fact that, as I've repeated at the outset, most of my constituents don't know what the laws are. They know there are rights, but they don't know what they are. There's a cost to this. I can agree with it, but we must know the cost.

I can concur that the government can provide better information, but you must have a fair idea too, because you're going to be asking specifically for increased staff.

I've finished; I'll leave it at that, Mr. Chairman.

**The Chair:** I think it is helpful. I'm wondering whether or not there's a middle road here. Public education seems to be very broad and could be very expensive. Public service can be something different. If there is a swarm of bank information problems—scamming through the Internet, or identity-theft type issues—about which the public needs to be engaged and cautioned, etc., this is public service, to me, because it's important to do, and it may help.

I think the points have been raised by the members about the costs. I would also hope, though, that to the extent that we get 100% operational on the investigations and the complaints side, all of a sudden the efficiencies can lead to opportunities to rejig resources as well and still stay within your envelope.

We will go to Mr. Siksay again, and then I have Mr. Wrzesnewszkyj and Mr. Kamp.

**Mr. Bill Siksay:** I'm sorry, Chair, I'll pass. My questions are done.

**The Chair:** Okay.

Mr. Wrzesnewszkyj, you have five minutes.

**Mr. Borys Wrzesnewszkyj:** Thank you, Chair.

I'd like to follow along the line of questioning that Mr. Dreeshen was following.

The RCMP is among the departments that have the largest number of complaints. When we drill down into the numbers concerning Mr. Dreeshen's request, it appears that five, two, and three have different categories wherein there are so-called “well-founded” complaints; another nine were resolved in process, but it appears that there may have been legitimate concerns in those nine. So we're up to about 14 out of the 52, which is about 27%, more than one out of every four.

When a department has the largest number, I would arrive at the opposite conclusion: that it's a worrying number, especially when you take into account the types of complaints we may be dealing with. The RCMP does criminal investigations. That sort of information, if not well founded—but it's been well founded that it has been made public or passed on to the wrong parties—can be incredibly damaging, even if it's in one case. It can be incredibly damaging to the future of an individual when shared with foreign governments. We saw what happened with Mr. Arar, yet the RCMP tells us we don't need any controls in place because they take a “principled” approach.

We have found out that they shared information over 3,000 times with foreign governments, other than with Interpol. We know that one of those governments is Sudan's. My goodness, its president has been indicted by the International Criminal Court for crimes against humanity. We know that information is being passed on to criminal regimes.

The RCMP has the capacity to garner information of a type that no other government department really has, besides perhaps CSIS. As I said earlier, there's genetic information, biometrics, using GPS, real-time video surveillance of which people are not aware—it's not like Street View, but stuff you're not aware of. But they take a “principled” approach. Canadians have paid a terrible cost by not having these regulations in place.

But that's dealing with foreign governments. What about what's happening in-country, in Canada? A book just came out—and this really worried me—by a staff sergeant, a former RCMP officer, in which he quotes one of our former commissioners as saying that approximately 30 parliamentarians were under investigation.

We know that in the fall of last year, one such individual's privacy—Mr. Casey's—was affected when an ATIP request was released with all names removed except his in one particular spot. That can be incredibly damaging to a politician, just the nuance that there may have been a criminal investigation—notwithstanding the fact that in this particular case there was no basis for it. But they tell us we don't need these recommendations to be enacted, because they take a “principled” approach.

Consider Glen Clark, the former premier of British Columbia. The media were called as the RCMP arrived in the middle of the night, and he was caught like a deer in lights. You saw him opening up the door to his house. His career was extinguished at that moment. He's been exonerated, but there is no going back.

What about the RCMP having regulations in place to prevent that sort of situation occurring—or during an election campaign? Would you recommend—

• (1700)

**The Chair:** You've taken four and a half minutes already.

**Mr. Borys Wrzesnewskyj:** So I have half a minute to ask the question.

**The Chair:** No, it's for questions and answers. You understand.

**Mr. Borys Wrzesnewskyj:** Okay.

Would you recommend, taking into account the track record, the ability to gather information of a type that most other departments cannot, and the nature of the department—a paramilitary department that's supposed to be there for law enforcement—or would you not recommend that there be additional recommendations to particularly target the RCMP, to make sure that these grave concerns to our own democracy and the human rights of Canadians who travel abroad are not violated?

**Ms. Jennifer Stoddart:** Can I ask Madame Bernier to answer? She is the former Assistant Deputy Minister of Public Safety, so it's an area she knows well.

**Ms. Chantal Bernier (Assistant Privacy Commissioner, Office of the Privacy Commissioner of Canada):** I would say your statement really underscores our position in relation to information-sharing agreements and to ensure the Privacy Act is more specific in that regard. And what you say has also been the object of the O'Connor report, where Justice O'Connor specifically requires that a much stronger framework apply to information-sharing agreements to ensure the protection of privacy, to ensure that information that is shared is accurate, as well as to make sure that personal information is not shared with states that do not have a human rights record, and that is precisely what we put forward. To contrast law and policy, as the commissioner has said, Treasury Board Secretariat has issued guidelines that seek very much to address these recommendations, and yet in our 2003-2004 report we found quite a few deficiencies, looking at information-sharing agreements.

For example, the information to be shared as described in the information-sharing agreements was far too general. The protection clauses, meaning how the information was going to be secured once shared, were also very vague. We also found that only half the agreements contained a third-party caveat, meaning once we give it to one party, it cannot share it with a third one.

The majority of the agreements did not provide for consistent use, meaning the information could not be used in a way different from the objective it was shared for. And finally, the vast majority did not contain an audit provision. So, absolutely, we are in complete agreement as to the necessity to have stronger provisions in the Privacy Act in relation to information-sharing agreements.

**The Chair:** Okay, thank you. It brings back Bill C-6.

Mr. Kamp, please.

**Mr. Randy Kamp (Pitt Meadows—Maple Ridge—Mission, CPC):** Thank you, Chair.

Welcome, and thank you for your efforts in working to help balance the rights of individuals and yet help us maintain our responsibility as parliamentarians, particularly with regard to issues of whether it's balancing personal and national security concerns.

In recommendation nine, you ask for the introduction of the provision regarding a five-year parliamentary review. Regretfully, I haven't spent any time on this committee, but I'm just wondering where this five years came from. Is that an arbitrary figure? Should it not be an ongoing procedure? Should it not almost be yearly rather than necessarily at five years? The world is changing so dramatically. We run into so many circumstances that could alter the provisions we have right now, whether it's cyber-terrorism, whatever. Why did you come up with the five years, and how comprehensive would you like to see this review be, and who should the participants be and how binding should it be?

• (1705)

**Ms. Jennifer Stoddart:** The five-year review comes from precedent. Because we have the temerity to label these quick fixes—we know there are no quick fixes in a parliamentary process that involves so many actors and so on—we tried to hone in on things that were perhaps easy, understandable, and for which there was a precedent. So we looked at the other law we administer, the private sector law that applies to banks, airlines, organizations, and provinces that don't have their own private sector privacy legislation, and there is a five-year review there.

In some of the other provincial legislation, there are five-year reviews too. In B.C., Alberta, I'm not sure about Ontario, but certainly Quebec, the legislation comes up automatically for review. The scope of the review depends on the parliamentary committee that's reviewing it. The legislation just says that so the committee can do an in-depth or a perhaps shorter review depending on that, and then it would make recommendations. But I have not seen any legislation that says the recommendations would be binding on anyone. They follow the normal parliamentary process.

**Mr. Randy Kamp:** How privy are you to national security concerns in your deliberations?

**Ms. Jennifer Stoddart:** I'm not directly privy very often to the details of national security concerns. Some of our investigators have a high level of security clearance, and when there are complaints for classified information they may look at it to the extent they understand that, but that's fairly exceptional.

**Mr. Randy Kamp:** I'm just wondering, because there are obviously some very serious security concerns at times, and I just wonder where that balance comes in between your responsibility to investigate circumstances where privacy can be breached and of course the necessity for the government and the state to protect the rights of its individuals. I just didn't know how far along that slope you go, and where the final decision-making sits as to what you are allowed to have and what you're not. Could you elaborate?

**Ms. Jennifer Stoddart:** Well, obviously, if it's sharing information and a government department doesn't want to share the information and doesn't, we're kind of stuck there, I would say. But I'd say we do have the confidence of the government under our act to see quite a bit of national security legislation.

We're just finishing up a legislated mandated audit of FINTRAC, which involves understanding the FINTRAC processes of anti-money-laundering legislation. We looked at CSIS, I believe, last year. As I said, we went into the RCMP exempt banks.

So from time to time, on specific issues, yes, we do see national security concerns.

**Mr. Randy Kamp:** It is a concern as well, from some particular point—having had some involvement in security over the course of my life—that if you have a contact where there has been 20 years' worth of work to build that source, and millions and millions of dollars invested in that, and then we have information that may or could or should be delivered for the purpose of the preservation of the privacy of an individual, where do we draw that line? That's sort of where I wonder where you come in on this.

**Ms. Jennifer Stoddart:** Perhaps my colleague, who has worked in this area for a long time, could add something.

**Ms. Chantal Bernier:** The Supreme Court of Canada has drawn that line of balance between privacy and safety. That line is about necessity. So the information that is collected must be necessary to serve the public safety objective it serves, as well as proper attention to the reasonable expectation of privacy. That is contextual, and the context will determine how the intrusion is valid or not.

We need, in the area of national security, to exercise a certain amount of deference for the very reasons that you invoke. The courts have stated as much. In our thinking we apply the principles that have been issued by the Supreme Court of Canada and other tribunals in Canada.

• (1710)

**Mr. Randy Kamp:** Thank you.

**The Chair:** Mr. Kramp, Ms. Block was hoping to get another...

**Mr. Randy Kamp:** Okay.

Thank you.

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

I might have some time that I could easily give back to Mr. Kramp, if he would like.

I am specifically looking at recommendation two and recommendation six. In addition to the conflict that these recommendations appear to pose, does the requester not already have recourse under

the Privacy Act if the Privacy Commissioner refuses or discontinues a complaint?

**Ms. Jennifer Stoddart:** Yes. The seeming contradiction between recommendations two and six is another attempt to balance the use of public funds in investigations, which are very labour-intensive operations, and justice for the Canadians who come to us with their privacy complaints.

Actually the commissioner and complainants can go to Federal Court, but only in the very limited circumstances of being refused access to one's file. If there are corrections to be made in one's file and the government department does not want to carry them out, then there's no further recourse. There's also the whole issue of damages. I believe some of the members of this committee have talked about that just now. If the actions of a government agency in the use of your personal information cause you damage, there is no recourse. That is one of the reasons I think it would be a timely amendment to give you that right to go to Federal Court. In the private sector, if an organization misuses your personal information—for example, a bank—and causes you some damage, you can go to Federal Court and have a remedy. Now Canadians who have their personal information misused by the government have no effective remedy. They can just have access to their file and that's all. That's recommendation two.

Recommendation six tries to make the act more contemporary, more focused, and to give my office the power to concentrate on the complaints for which there has not already been a determination, for which we can really do something and help the individuals. For instance, we have many complaints about the same things. For example, why does Canada Revenue Agency take all this personal information; this must be against the Privacy Act. If our powers were changed, then we'd like to say that we're not going to deal with this complaint because we deal with it several dozen times a year over the years, and here are all the examples. We'll tell people that we're not really going to investigate this; we're going to discontinue it because they basically have to give their personal information to the tax authority. That's a frequent source of complaint. We can then concentrate on other issues. For example, on recent issues with Canada Revenue Agency, perhaps there had been some misuse of the personal information within the department and some employees had overstepped their bounds of duty in looking at tax files when they shouldn't, and things like that.

The two may seem to be contradictory, but they work into this kind of more targeted approach to the problems we see coming to us at this particular time.

**Mrs. Kelly Block:** I have one last question with regard to recommendation eight, which is to strengthen the annual reporting requirements of government departments and agencies. By requiring these institutions to report to Parliament on a broader spectrum of privacy-related activities, would this mean legislating Treasury Board guidelines, which could compromise their flexibility?

•(1715)

**Ms. Jennifer Stoddart:** No. In fact I think it's the inverse. It's taking a lot of the information in Treasury Board guidelines and simply bringing it up to the status of a law. Treasury Board could then issue new directives of interpretation of the law. Again, it's because we're trying to put forward practical things that are already in existence, but we simply want to increase compliance with them.

**Mrs. Kelly Block:** Thank you.

**The Chair:** Very quickly, I'd like to speak about recommendations 11 and 12.

These are existing policies. I'm a little concerned that if you were to bring into legislation existing Treasury Board policy, you'd have to change a whole bunch of legislation because of a difference in force or effectiveness. Is it necessary? Should it be just in the regulations, or is it something that has to be mentioned that of course this legislation is to comply with all Treasury Board guidelines as they bring change from time to time? How important is it? You have to fight for these two, quite frankly. Is this going to make the act a better act at the level of a quick fix, or is this just, by the way, we can maybe do a little amendment here?

**Ms. Jennifer Stoddart:** No. I think this is essential.

One dimension that I haven't mentioned today is the international dimension of Canada as we look around the networked world and see that Canada is becoming one of the few modern countries that really hasn't touched up its national privacy legislation. Right now, your European colleagues in the European parliament are adopting data breach notification under European law.

So the fact that we don't have this, the fact that we don't have many of these provisions even though they exist in directives, dims Canada's lustre internationally, whereas Canada was once a leader in this field.

**The Chair:** Okay.

**Ms. Jennifer Stoddart:** It's being done all over the world now.

**The Chair:** So incorporation by reference isn't going to get far enough for you?

**Ms. Jennifer Stoddart:** Not ideally: I think it takes a little drafting.

**The Chair:** All right. I do understand.

I think, Commissioner, we saw this in Bill C-6, the health bill on human pathogens and toxins, where information could be shared with foreign governments, but the conditions were vague, it could be passed on again, and there were no conditions on how long that information could be kept. It really gets a little convoluted when you get those kinds of things happening.

We'll certainly be commenting on numbers 11 and 12, even though we haven't had witnesses to give us much input. As usual, you've acquitted yourself very well, I think, with your colleagues, in presenting your views on these things to help us better understand where you'd like to go with this.

You're an officer of Parliament and you're charged with a significant responsibility on behalf of Canadians. We know that you're here with the best interests of Canadians at heart, so we thank you kindly for that input.

The committee would like to meet in camera for a short while, so I'm going to excuse you now.

**Ms. Jennifer Stoddart:** Thank you very much.

**The Chair:** We'll just suspend until we can convert over.

*[Proceedings continue in camera]*

---





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

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

**Also available on the Parliament of Canada Web Site at the following address:  
Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante :  
<http://www.parl.gc.ca>**

---

**The Speaker of the House hereby grants permission to reproduce this document, in whole or in part, for use in schools and for other purposes such as private study, research, criticism, review or newspaper summary. Any commercial or other use or reproduction of this publication requires the express prior written authorization of the Speaker of the House of Commons.**

**Le Président de la Chambre des communes accorde, par la présente, l'autorisation de reproduire la totalité ou une partie de ce document à des fins éducatives et à des fins d'étude privée, de recherche, de critique, de compte rendu ou en vue d'en préparer un résumé de journal. Toute reproduction de ce document à des fins commerciales ou autres nécessite l'obtention au préalable d'une autorisation écrite du Président.**