House of Commons
CANADA

Subcommittee on Public Safety and National Security of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness

SNSN • NUMBER 014 • 1st SESSION • 38th PARLIAMENT

EVIDENCE

Wednesday, June 1, 2005

Chair

Mr. Paul Zed

Subcommittee on Public Safety and National Security of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness

Wednesday, June 1, 2005

● (1835)

[*English*]

The Vice-Chair (Mr. Kevin Sorenson (Crowfoot, CPC)): I call this meeting to order, pursuant to the order of reference of December 9, 2004, a study of the Anti-terrorism Act by the Subcommittee on Public Safety and National Security of the Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness, meeting number 14.

We are pleased this evening to have with us Ms. Jennifer Stoddart, the Privacy Commissioner; Raymond D'Aoust, the Assistant Privacy Commissioner; and Patricia Kosseim, general counsel. Welcome here again.

We apologize for these votes, which have kind of shortened the evening, but we look forward to your comments.

The floor is yours. If you know the process, as I'm sure you do, you can have opening comments, and we will go through the questions and answers.

Ms. Stoddart.

Ms. Jennifer Stoddart (Privacy Commissioner, Office of the Privacy Commissioner of Canada): Thank you very much, Mr. Chair. We're very happy to be here on this important issue.

You have our submission. I also have quite extensive prepared remarks today, which I will not go through completely.

[*Translation*]

I will review the highlights of my opening statement and members can follow up with questions.

[*English*]

The remarks today will be focused primarily on what seems to us to be the lack of facts and evidence uncovered so far to suggest that the measures provided for by the Anti-terrorism Act are necessary. We urge you, through your deliberations, to critically assess the issue of proportionality in the law and consider a number of our proposed practical recommendations to address the impact of these measures on privacy rights.

[*Translation*]

I will start with some general comments on anti-terrorism and privacy rights.

No one denies the reality of the threat that the Act was intended to address. We must ask ourselves, however, whether what we gain from the Act in security justifies the sacrifice of privacy and other rights. Regrettably, there appears to exist no empirical evidence shared with Canadians to suggest that the measures provided for by the Anti-terrorism Act are necessary. This is one of the paradoxes of the present exercise and it prompts my first comment to you that this Act should be subject in its entirety to a recurring sunset clause. We suggest that the Act should be reviewed every five years. That would be a kind of recurring sunset clause.

Specifically, the impact of the Act can be grouped into three broad themes. First, the surveillance powers of security and intelligence and law enforcement agencies have been overly broadened. Second, constraints on the use of those same surveillance powers have been unduly weakened. Third, government accountability and transparency have been significantly reduced.

Regarding the first theme, the Canadian government has introduced a series of measures to broaden its surveillance powers. The Anti-terrorism Act has set the tone for creating a broader net for surveillance of organizations and individuals. As you know, it was accompanied by changes to the Aeronautics Act, the Public Safety Act and PIPEDA. It will soon be followed by “lawful access” proposals. Much of the personal information gathered is highly sensitive and part of integrated information systems that could impact the lives of Canadians if the information were misused, distorted or misinterpreted.

However, public opinion trends, including a recent poll by my office, suggest that Canadians are increasingly aware of informational privacy issues and expect a reasonable and balanced approach to a national strategy to combat terrorism. The poll shows there is strong support by the public for greater accountability, transparency and oversight of agencies involved in national security.

There is a real risk that as the logic of anti-terrorism permeates all spheres of law enforcement and public safety, large-scale systems of surveillance will increasingly erode privacy rights in Canada, without a critical assessment of where it is appropriate to draw the line. ID cards, uncritical use of new technology, such as RFIDs, increased data mining and integrated law enforcement systems are other looming threats to privacy.

[*English*]

At the same time as the surveillance powers of the state have been strengthened by the Anti-terrorism Act, constraints on those powers have been weakened. We see that law enforcement and national security agencies are no longer required in anti-terrorism investigations to consider other investigative methods prior to applying for judicial authorization for electronic surveillance. The executive branch of government may displace the role of the judiciary in issuing security certificates and in authorizing interception of communications, and the judicial standard of reasonable grounds to believe has been lowered to one of reasonable grounds to suspect.

A number of the amendments in this act have had the effect of weakening independent oversight of the surveillance activities of law enforcement and security and intelligence agencies. We feel that independent oversight is one of the pillars of democratic freedom, and so the question of who watches the watchers is best answered by ensuring oversight of the surveillance powers of the state by the judiciary and other independent agents. Parliament and Canadians need to question the measures in the Anti-terrorism Act that reduce oversight. Independent review should be the rule, not the exception.

I'd like to talk now about our concerns about decreased government transparency.

Amendments brought about by this act have also added to the secrecy surrounding legal proceedings, contrary to the fundamental principles that court hearings should be conducted openly, and that individuals should be entitled to know the charges against them and the evidence relevant to the charges.

Among the most significant changes affecting transparency and access of individuals to their own personal information are the various amendments to section 38 of the Canada Evidence Act, the section that addresses the judicial balancing of interests between the public interest in disclosure and the interest of the state in national security and maintaining foreign confidences. As amended by the Anti-terrorism Act, section 38 of the Canada Evidence Act provides a broad statutory gag order that prohibits not only the disclosure of the information itself, but also the mere fact that section 38 proceedings have been engaged. We feel that these restrictions on disclosure are in many cases overly broad.

The Anti-terrorism Act further amends, as you know, section 38 procedures by permitting the Attorney General to override a Federal Court order that information should be disclosed. This extraordinary power is, we feel, unnecessary in view of the judicial rigour that already exists under the Canada Evidence Act, which appropriately allows a judge to determine the balance of the competing interests between disclosure and national security.

In my presentation, Mr. Chair, we resume the 18 recommendations that we make and try to group them according to general themes.

I'd like to go on to bring to your attention our recent work on the transfer of personal information to foreign government agencies. In response to the concerns of Canadians about where their personal information is going, and particularly where it is going when it crosses borders, my office has launched a major audit of the Canadian Border Services Agency, which, as you know, is an integral part of the PSEP portfolio. The objective of this audit is to assess the extent to which the Canadian Border Services Agency is adequately controlling and protecting the flow of Canadians' personal information to foreign governments or institutions thereof.

The premise of this audit is that national security objectives and sound personal information practices are mutually dependent. Underlying this hypothesis is the belief that strong controls over the handling of personal information will limit privacy risks such as improper uses or disclosures, which will also support a robust national security framework. Collection, use, and disclosure of personal information must be limited to that which is necessary and permissible by law, and should be circumscribed by multiple layers of privacy and security protections during its entire life cycle to prevent and mitigate risks that may impact equally on personal privacy as well as on national security objectives.

The audit will examine several key operational systems used to process personal information collected, processed, and shared by the Canadian Border Services Agency with U.S. counterparts. The audit will, we hope, also assess the overall robustness of the CBSA's privacy management regime, as well as how it reports on its privacy management responsibilities to Parliament and the public.

● (1840)

I would draw your attention, Mr. Chair, and the attention of the honourable members then to the description in the pages that follow. I have an integrated version.

[*Translation*]

I cannot give you the exact page numbers in the two versions, but our discussions with the President of the Treasury Board which focused on our concerns about privacy protection within the federal government are summarized over three or four pages. This specifically concerns recommendation 15.

[*English*]

So the pages that follow are an update since we wrote our submission on the development of an appropriate privacy management framework for the circulation of personal information within the federal government, including issues that have to do with the contracting out of personal information and U.S.A. PATRIOT Act issues. Those are on the four pages that follow.

The Vice-Chair (Mr. Kevin Sorenson): And they are pages 13, 14, and 15. Is that the recommendations you made?

Ms. Jennifer Stoddart: Pages 17 to 21 in the English version.

● (1845)

The Vice-Chair (Mr. Kevin Sorenson): Do we have those?

Ms. Jennifer Stoddart: They're in your version, Mr. Chair.

The Vice-Chair (Mr. Kevin Sorenson): Wrong pages, but they're the recommendations?

Ms. Jennifer Stoddart: You don't have that text? I didn't want to take up more than my allotted time in going through them.

Mr. Tom Wappel (Scarborough Southwest, Lib.): I'm sorry, Mr. Chair, what are we referring to? I don't have those pages.

The Vice-Chair (Mr. Kevin Sorenson): Yes, we have nothing of pages 16 and 17.

Ms. Jennifer Stoddart: This is my opening statement, Mr. Chair. I'm sorry, it's not the substance of my submission.

The Vice-Chair (Mr. Kevin Sorenson): We have your opening statement. Is that what you're making reference to?

Ms. Jennifer Stoddart: Yes.

Mr. Tom Wappel: It only goes to page 15.

The Vice-Chair (Mr. Kevin Sorenson): I see. All right, wait a minute.

This is the one that I think I read from earlier here. This is the position statement on anti-terrorism. That is not the same as what was circulated here today, but it does go to page 25.

Mr. Tom Wappel: Excuse me, Mr. Chair, I have two documents. One is entitled "Position Statement on the Anti-terrorism Act", and that's dated May 11. That was when you were going to be here the last time. That's up to page 25.

Ms. Jennifer Stoddart: Right, that's our brief.

Mr. Tom Wappel: I also have "Opening Statement, Privacy Commissioner of Canada", dated June 1, and my version goes up to page 15 and it ends at recommendation 18. Is that what you have, Mr. Chairman?

The Vice-Chair (Mr. Kevin Sorenson): That is the same as what the chair has.

Ms. Jennifer Stoddart: I'm very sorry, Mr. Chair. The version you should have goes to page 24 of the opening statement, plus the recommendations.

[*Translation*]

You'll find it on page 26 in the English version.

[*English*]

The Vice-Chair (Mr. Kevin Sorenson): We don't have it.

Ms. Jennifer Stoddart: Should I read it into the record then, in the absence of that?

The Vice-Chair (Mr. Kevin Sorenson): How many pages is it?

Ms. Jennifer Stoddart: It's three or four. Or we could send it to you.

The Vice-Chair (Mr. Kevin Sorenson): I think you should send it. If you're going to make reference to what is in there, it might be advantageous to us that when you are referencing the extra pages you let us know. Otherwise, we're going to be scrambling to find something we don't have access to. I don't think it has to be read into the record. If you would forward that on to the clerk, that would suffice.

Ms. Jennifer Stoddart: Yes, we will.

The Vice-Chair (Mr. Kevin Sorenson): Do you still have more in your opening statement?

Ms. Jennifer Stoddart: I simply wanted to go to my conclusion, then, which I think is the same—I hope—as in the one the previous opening statement. I think we changed our opening statement from our original date for appearance.

The Vice-Chair (Mr. Kevin Sorenson): And that's not a big deal. What you give as an opening statement into the record many times is not exactly the same as what we're given. You can take great liberty with your opening statement. So if you want to conclude with your remarks, go ahead

.

Ms. Jennifer Stoddart: I could go to the conclusion, which I believe is largely the same on whatever page you have—I hope.

We would like to draw to your attention, then, Mr. Chair, that this act you are reviewing reflects a fundamental shift in the balance between national security, law enforcement, and informational privacy. There has been, over the last few years, an associated loss of privacy and due process protection for individuals.

Overly broad state powers in the name of national security may in fact imperil the self-identity of democratic nation states. It is imperative that the means and measures adopted to combat security threats do not end up abrogating the very freedoms that define and give substance to the democracy we claim to be defending. This is not a new statement, but it's an important one, I think.

Contrary to what is sometimes thought, security and the protection of informational privacy need not be seen as a trade-off, where one is necessarily sacrificed in the interest of the other. We feel both can be achieved, with well-designed law, with prudent policy, and effective but not excessive oversight.

I urge the subcommittee gathered here today to carefully consider our remarks and recommendations. We hope this will help you achieve the goal with which you've been entrusted.

This is the summary of our remarks. I apologize for the confusion in the versions. We'd be happy, Assistant Commissioner Raymond D'Aoust and I, to talk to the pages you didn't have. We would be happy to answer your questions.

● (1850)

The Vice-Chair (Mr. Kevin Sorenson): Thank you, Commissioner.

Yes, if you can get those.... We weren't sure if we should really ask for the papers. We thought maybe it was something we didn't have to know and that was maybe private.

Mr. MacKay.

Mr. Peter MacKay (Central Nova, CPC): Ms. Stoddart, welcome to you and to your officials. We very much appreciate your presence here and your very fulsome presentation.

I've broken down your critique of the act into three general areas. You are concerned over the gains in security versus the sacrifice on the privacy side, and much of that, I think, comes from the surveillance ability that is empowered in the security intelligence and law enforcement agencies now.

You also talk about the constraints on those surveillance powers now being weakened.

The third element that I glean from your presentation is the one I'm most concerned about. That is the overall perception or reality of government accountability and transparency being reduced. To that end, one of the recommendations you make—I believe it's recommendation number eight—centres on the diminution of basic information in privacy rights under section 38 of the Canada Evidence Act. You've made a number of suggestions related to that section.

My first question is whether it is your view that amendments in the act that came about as a result of the anti-terrorism bill do not go far enough to protect Canadians' rights under the Privacy Act, and that the ability of your office is also limited; that you feel the office doesn't have the same powers that existed prior to the enactment of Bill C-38.

Ms. Jennifer Stoddart: Thank you for the question, honourable member.

I think one of the interesting and possibly ironic features of this act is that it changes the Privacy Act and the other act for which we have responsibility—PIPEDA, the Personal Information Protection and Electronic Documents Act—slightly but significantly in that it allows, under PIPEDA, private companies to become in essence agents of the state. That is, travel agents can be asked to glean information and pass it on to the state.

There is a change under the Privacy Act that says that if we are investigating something on a complaint that has national security implications, we can be served with a certificate. That change to the Privacy Act has not been used, and of course we have no reading on how the PIPEDA disposition is working.

I say it's ironic, honourable member, because I think one of the major problems is that the Anti-terrorism Act didn't have to change the Privacy Act very much, because the Privacy Act is a very weak standard already and was in a state, I would say, of growing irrelevance in terms of adequate standards for protection of personal information by international standards at the time the anti-terrorist legislation came in.

So this act does not have a huge impact on the Privacy Act. The issue, I think, and an issue that we bring up—and I believe it's one of our recommendations and one I've been talking about—is that Parliament should look to reforming the Privacy Act in itself and bring it up to a more acceptable standard.

Mr. Peter MacKay: This flows into my next question. You're critical of the security provisions in the act, and you suggest the security imperatives do not really permit information to be disclosed at times. I take it from your recommendation that you feel a special advocate injected into this system might help rebalance this equation. What I immediately thought was, why wouldn't the Privacy Commissioner herself—or himself—be able to play that role, or even the Information Commissioner be able to undertake that type of activity? I'm concerned from a practical standpoint as to why we would want to create another office for that particular role. Is there some pressing need to have, for example, a judge fill that role as the special advocate?

● (1855)

Ms. Jennifer Stoddart: No. I believe some critics have in fact suggested that this would be possible. If Parliament were to name us to play that role—presumably, as information commissioners we already exist in law and so on—I don't see why we couldn't.

Mr. Peter MacKay: So your current mandate could be expanded to include that.

Ms. Jennifer Stoddart: We would have to, I would think, have that under a change in law. We would also have to have—which is another issue about our role in looking at the extent to which Canadians' personal information rights are compromised by any anti-terrorist legislation—some specific resources in order to be able to fill that mandate.

Mr. Peter MacKay: Your comment with respect to passenger lists and tourism are very timely because, as you may be aware, American officials are requesting that Canadian passenger lists be disclosed whether the planes are going through the United States or not. I'd like to give you an opportunity to give us your view, on the record, of that request, and I invite you to share that recommendation with us and all Canadians.

Ms. Jennifer Stoddart: Certainly my office has been following the possibility of having no-fly lists, which would be applied to Canadians and would impinge on their being able to go from one part of our country to another, with great interest over the last few months—more than that, a year or a year and a half. Unfortunately, we have very little information. We know that no-fly lists are being developed by the Department of Transport for application within Canada and we periodically attempt to assess the state of development of these no-fly lists, but so far we have no information. We're concerned about how they could be developed, how they could be used, whether they respect the spirit of the Privacy Act, and so on.

Mr. Peter MacKay: What's your general reaction, though, to that request, should it come from the Americans, that they want that information disclosed?

Ms. Jennifer Stoddart: Well, my reaction is to ask, to what agreement would it be pursuant, to what law? I think we'd have to look at that. How is it getting the information on Canadians, and do we as the Canadian government provide this information to them within the spirit and the letter of our own laws? That's why we're doing the Canada Border Services Agency audit. Clearly, we have no jurisdiction over foreign entities, but we can see that we observe our own laws in terms of the information we're sharing abroad. I think that should be looked into very carefully in all cases.

The Vice-Chair (Mr. Kevin Sorenson): Thank you,

Monsieur Ménard.

[*Translation*]

Mr. Serge Ménard (Marc-Aurèle-Fortin, BQ): Thank you.

I'd like to ask you, first of all, if your Office has the required resources to do a full independent review of how anti-terrorism activities carried out by security and intelligence enforcement agencies impact privacy.

Ms. Jennifer Stoddart: Absolutely not.

Mr. Serge Ménard: Consequently, you have not been able to carry out this review.

Ms. Jennifer Stoddart: No.

Mr. Serge Ménard: However, you've already done an outstanding job in terms of examining. Is this something that you would like?

Ms. Jennifer Stoddart: Are you asking if we would like more resources?

Mr. Serge Ménard: Yes, I'm asking if you would like additional resources to study the act and the potential conflicts with privacy issues.

Ms. Jennifer Stoddart: We would.

Perhaps I should bring you up to date on our budgetary situation. I explained the situation in some detail to another parliamentary committee yesterday in conjunction with the consideration of the estimates.

● (1900)

Mr. Serge Ménard: By all means.

Ms. Jennifer Stoddart: The resources allocated to us under the Privacy Act have not changed since 1997 or thereabouts. In this, the new era that dawned in 2001, we are largely overwhelmed and unable to monitor closely the circulation of personal information. We are currently doing some studies with a view to requesting more operating funds from Treasury Board this summer. We do not even receive any permanent funding to administer the new act, PIPEDA. All of these operations must be consolidated.

Although we don't know if we'll get the funding we are seeking, we do plan to ask for a substantial increase in resources for our audit activities. We're only talking about a few audits here, because I don't imagine that we'll audit all operations. Is that our responsibility, or should it fall to an oversight body or to a parliamentary committee? Our current mandate calls for us to do at least a few random audits.

Mr. Serge Ménard: I see.

You stated the following in your opening remarks, and I quote: Regrettably, there appears to exist no empirical evidence shared with Canadians to suggest that the measures provided for by the Anti-terrorism Act are necessary.

The truth of the matter is that since the very beginning of these hearings—I believe this is our 13th or 14th meeting—we have continued to hear witnesses rationalize the existence of this Act through repeated references to the most tragic of events, without really explaining to us how the proposed legislative provisions would have prevented these tragedies from occurring in the first place.

Is that what you meant by your reference to the lack of empirical evidence?

Ms. Jennifer Stoddart: In part, yes.

On the other hand, on reading some of the testimony that was presented to the committee, we were struck by the absence of any factual accounts, even of a general nature.

We understand that we're dealing with national security issues, but we mustn't be naive either. Nevertheless, it's difficult for members of the public, who do not make up the country's security forces, to truly understand in any objective, concrete way the extent of the threat . Getting back to this essential principle of law that applies when we interpret rights and freedoms: are the proposed measures in proportion with the risks we face?

There are many different opinions on this subject and various people claim to have different requirements. We know that groups sympathetic to terrorists are very active, but it's very difficult for the public to appreciate this reality. I believe that's what is meant by the lack of “empirical evidence”.

Mr. Serge Ménard: However, since you did conduct a number of public opinion polls—as did other groups which shared their findings with us—I trust you realize that overall, the public acknowledges the threat of terrorism. Witness the events in Bali, in Spain and the 9/11 attack. Therefore, it's important to take some kind of concrete action. However, there is no evidence to prove that these tragedies might have been averted had these powers already been granted.

Ms. Jennifer Stoddart: That's correct.

Mr. Serge Ménard: Did you also look for some evidence?

Ms. Jennifer Stoddart: We did. Moreover, many critics maintain that the aim of the legislation is to facilitate the work of intelligence agencies. However, because we are not experts in that field, we will hold our comments.

Mr. Serge Ménard: In fact, we're often told that in future, it would be useful to have the power to compel people to disclose information, and the mandate to interrogate individuals. However, these are not really your Office's concerns.

Ms. Jennifer Stoddart: No, these are more in the nature of criminal law considerations and a question of fundamental freedoms. The Act does provide for preventive detention and individuals can be interrogated pursuant to the Criminal Code and other relevant acts. The question is, can persons be compelled to tell the truth?

● (1905)

Mr. Serge Ménard: Yes, but they cannot be tortured.

Ms. Jennifer Stoddart: Correct.

Mr. Serge Ménard: When people are tortured, they ultimately end up saying what they believe the person inflicting the torture wants to hear.

Obviously, privacy information is also gathered by electronic means and this troubles you as well.

Ms. Jennifer Stoddart: That's correct.

Mr. Serge Ménard: Are you familiar with the measures taken to ensure that access to information pertaining to investigations is limited and such information disclosed only when absolutely necessary, for example, when investigators from foreign, friendly nations, wish to conduct investigations here in Canada? Are you familiar with the measures taken to ensure that electronic information isn't simply downloaded to foreign databases? They may be friendly nations and we may be united in the same struggle, but...

[*English*]

The Vice-Chair (Mr. Kevin Sorenson): Could we have Ms. Stoddart, and then Mr. Comartin.

[*Translation*]

Ms. Jennifer Stoddart: No. Our job does not include being familiar with such procedures and processes, if they do in fact exist. One component of our Office's mandate is to conduct polls or random audits to ascertain if the procedures employed to transfer information are in compliance not only with the Act, but also with specific agreements between countries on the sharing of information.

We did do a partial evaluation of RCMP units assigned to handle transborder situations. We also discussed information sharing in our latest annual report. That's as far as we've been able to go until now.

[*English*]

The Vice-Chair (Mr. Kevin Sorenson): Thank you, Madam Commissioner.

Just before Mr. Comartin asks his question, may I ask if it would be all right with you, Madam Commissioner, if we extend our time? We were about a half an hour late starting. Is your time available?

Ms. Jennifer Stoddart: We're here at the disposal of the committee. We're an agent of Parliament. However long you would like to keep us, we'll be here.

The Vice-Chair (Mr. Kevin Sorenson): That's always good to know. And how long we keep you depends on whether or not supper shows up.

Mr. Comartin, go ahead, please.

Mr. Joe Comartin (Windsor—Tecumseh, NDP): Thank you for coming, Madam Commissioner.

I think maybe because of the missing pages, I just want to be clear on what has gone on here. Is the audit you're doing on the Border Services Agency under way now?

Ms. Jennifer Stoddart: Yes.

Mr. Joe Comartin: Okay.

Are the methodologies that you're deploying to do that audit significantly different from what you would want to use under the privacy management framework and the work that you want done under that in...I forget which recommendation it is now. I'm not sure what methodology is being recommended and/or used. Is what you're doing with the Border Services Agency what you want done across the whole of the intelligence-gathering sector?

Ms. Jennifer Stoddart: I think generally. I'm not an auditor. Could I ask Commissioner D'Aoust to give you more information? He's perhaps closer to that question.

Mr. Raymond D'Aoust (Assistant Privacy Commissioner, Office of the Privacy Commissioner of Canada): The audit was launched a few months ago. We are now in the process of scoping and developing the terms of reference for this. We are having discussions with the Canada Border Services Agency on the terms of reference for this audit. So we're going to be looking at different systems, systems that share information with our U.S. counterparts, and at how this information is processed, how it is kept, and so on.

So the methodology then the officers are using are the typical audit methods, which include interviews with CBSA managers, site visits—we have already done a few site visits as part of the scoping exercise—and file review. So those are the methods we're using.

We're using a multiple lines of evidence approach, if you will, to make sure we can corroborate our findings through different sources of information.

In terms of the privacy management framework, this is a series of measures, sound personal information practices, if you will, that we believe the federal government should apply across the board. That includes having the systems in place to ensure that no information gets leaks to unauthorized sources.

● (1910)

Mr. Joe Comartin: Mr. D'Aoust, I'm sorry, just so I'm clear, this is what you would want for each of the agencies or departments?

Mr. Raymond D'Aoust: Correct.

Mr. Joe Comartin: And is there a model reduced to writing that you would want deployed in each one of those agencies or departments?

Mr. Raymond D'Aoust: We haven't defined this model. We are having discussions internally, but also with our colleagues from the Treasury Board in terms of defining this model. We certainly believe that minimally they should be complying with the spirit and the letter of the Privacy Act. That's a starting point. But we think we can go a bit further than that.

So the model is evolving as we speak. It includes also the carrying out and conducting of a privacy impact assessment.

Mr. Joe Comartin: That would be done by the individual agency and department?

Mr. Raymond D'Aoust: Correct, and we review those PIAs, privacy impact assessments, and provide comments and advise on strategies to mitigate privacy risks. So it's a series of measures of that nature.

Mr. Joe Comartin: So then, using that, would it allow you to make assessments and report to Parliament on whether in fact privacy is regularly being negatively impacted in any of the departments?

Ms. Jennifer Stoddart: Yes, that would be the intent. It would allow us to come up with some kind of report card.

Mr. Joe Comartin: And the information sharing that goes on internationally, which is obviously of concern, would it get at that? Would it be able to give us an assessment of how much is going out, whether privacy is being infringed at the international level because of those exchanges?

Mr. Raymond D'Aoust: That's more difficult to assess, to be honest. I'm not sure we would be able to get to that level of detail.

Mr. Joe Comartin: The model that you're talking about now you don't think would get us that information or that assessment, that analysis?

Ms. Jennifer Stoddart: It would probably depend on what you applied it to. You can audit the informational practices of many entities. It depends what those entities do and whether part of their mandate is to send information abroad or to conclude contracts.

But I wrote to the President of the Treasury Board in March and we just received a reply, which is the famous missing pages that we thought were relevant for this exercise. One of the things that I brought up was the issue of setting standards for the sharing of personal information of Canadians abroad.

We have not seen any standards. We have not seen any directives. Are there any directives when, for example, the Government of Canada concludes a contract with a private sector firm?

These are all questions, and the President of the Treasury Board replied that the government is actively working on this and we're going to be consulted, for example, on clauses for contracts for outsourcing data processing very soon.

So it depends on the configuration of the entity you're auditing as to what it does with the personal information. It may just circulate it within the department. It may share it between departments. It may send it to the private sector in Canada. It may send it to other Canadian governments and it may send it abroad.

Mr. Joe Comartin: Up to this point, including the response from the President of the Treasury Board, has the government, or any agency or department of the government, taken the position that, no, we're not going to do that, or no, you can't have that information because of national security considerations?

Ms. Jennifer Stoddart: I'm not aware of that. None has been brought to my attention. I don't know.

Mr. Joe Comartin: Mr. D'Aoust, up to this point with the audit of the Border Service Agency, you haven't met with any denials of information?

Mr. Raymond D'Aoust: No, thus far they've been very cooperative.

Mr. Joe Comartin: Okay.

The Vice-Chair (Mr. Kevin Sorenson): You have 25 seconds. Just ask the question, and we'll—

Mr. Joe Comartin: Okay, here's a quick one on your recommendation 13. Mr. Atkey's been appointed as amicus curiae to the Arar inquiry. Is that the type of work...? I don't know whether you've studied what his mandate is; it seems somewhat similar to what you're recommending in recommendation 13. Have you...?

● (1915)

Ms. Jennifer Stoddart: I haven't studied Mr. Atkey's mandate, but yes, it sounds similar to what.... I think it would be something similar; that is, someone who has a special role, who can see the documents that the person who is the subject of the legal proceeding couldn't, and therefore can help them defend their rights without seeing the impugned material.

Mr. Joe Comartin: I'm sorry, Mr. Chair, may I have just one more as a follow-up?

I've taken a look at his, and my sense is that the role you're proposing for this person—or as you describe him, “a security-cleared special advocate”—goes further than what his is, but I'm not certain of that.

Ms. Jennifer Stoddart: It could be.

Mr. Joe Comartin: You may want to be more specific.

Thank you, Mr. Chair.

The Vice-Chair (Mr. Kevin Sorenson): Thank you.

Mr. Cullen.

Hon. Roy Cullen (Etobicoke North, Lib.): Thank you, Mr. Chair, Ms. Stoddart, Ms. Kosseim, Mr. D'Aoust.

I know you're not bound by decisions or views of your predecessor, and in many respects I think that's a good thing. I was on the government operations and estimates committee when we dealt with Mr. Radwanski, and probably if he were here tonight, he'd say no, I have to go at 7:30. Anyway, we won't get into all that.

But in terms of privacy law and policy, it was generally understood that he had a reasonable grasp on it, and I notice that in 2001 on the Privacy Commissioner website he said that because of amendments to the Anti-terrorism Act in 2001: “All existing privacy rights of Canadians remain fully safeguarded, the oversight role of the Privacy Commissioner remains intact, and even the issuance of certificates is closely circumscribed and subject to judicial review”.

I'm wondering what has caused the change in thinking to where you argue that the anti-terrorism measures are overly broad and should be weakened and in fact argue that there's no empirical evidence that the measures are necessary in the Anti-Terrorism Act but, with respect, don't provide any empirical evidence to support your assertion that the terrorism measures are overly broad.

I'm wondering if there are two questions there, then: why the shift...? And these kinds of things can happen. You're not bound by Mr. Radwanski's views, but can you explain the shift? And what kind of evidence do you have to suggest that the anti-terrorism measures are overly broad?

Ms. Jennifer Stoddart: I think that's an important question: why would my views be so different from Mr. Radwanski's?

I think that takes us to the context in which as a society we adopted the Anti-terrorism Act. It was adopted very quickly, as I remember, although I wasn't working in the federal government at the time. It was adopted in a mere matter of months. We didn't know to what extent we would all be subjected to measures similar to those of September 11. I think as a society we saw the threat to our existence, to our security, to be immense.

Of course, the reading of one's reality always informs one's position. In that context, it may have seemed at that point.... Indeed, perhaps at that point in time we did get the mix right. However, as we've gone on, we have seen that some five years later that seems to be, certainly in North America, a rather isolated incident, from what the public can see. I come back to my remarks to the other honourable member about the lack of empirical evidence, for those who don't work in the security establishment.

Given that we have not been bombarded with a series of drastic incidents like that; given also that from what we can see the Canadian government itself has rarely used any of these powers.... We don't work in this area, but from what we see from critical comments, some of these powers have not been used at all, I think, and some are used very sparingly.

We're now as a society at a point five years later, and that's why at least we had the wisdom to say this takes a five-year review. Given that the circumstances are not as extraordinary as they may have seemed on the days following September 11, do we really need all these powers? Is this the best way to go in combating terrorism and security threats in a democratic society like Canada's?

I think we're now in a far different context. I've also been able to benefit from a lot of scholarship from many observers—many law professors and so on—who've looked at this. That was not available in 2001.

So I think that's perhaps our concern. We're very concerned that if, in circumstances that do not seem extraordinary, as they were in 2001, we go on with these extraordinary powers without seeming to have needed them, we inure ourselves to a basic change in the values of Canadian society. We become used to a bigger, more pervasive set of surveillance rules that do not bode well for privacy and freedom in the long term.

You also asked me the second question: do we have evidence? It's very hard for an organization like the Office of the Privacy Commissioner to gather evidence about the extent of terrorist activities. No, we have no evidence. We simply have the evidence that we can see that these powers have rarely been used. I think we have to turn the question on its head and say, given their extraordinary outreach, given their impact, given what it means for a democratic society to have such great surveillance powers, do we really need to go on with them?

If you decide—because you are the ones who are going to decide this, and you have heard other witnesses and may have access to information that we don't—that we must go on with these powers for the security of Canadians, we would urge you to make at least a change in the law that makes us go through this exercise every five years. As we read the law, there's a one-time sunset review. I think we need a recurring sunset review. We have to go through this regularly and ask whether we still need these powers: "Look at where we used to be; look at how far we've come. Should we not measure this distance? Do we still need to go that far?"

If there's one amendment you could make, I would urge that one on you.

● (1920)

Hon. Roy Cullen: Thank you.

Just by way of background, while Bill C-36 was dealt with fairly expeditiously in the House, there was a lot of thinking leading up to it. It wasn't as though this was a new idea just hatched in a couple of months. Nonetheless, I appreciate your point.

I'd like to come back to Peter MacKay's example. I'm not sure you understood—or maybe I didn't understand. I thought what Mr. MacKay was talking about.... There's been a story, and it's just what I've read in the press, where the United States is saying—let's say you're flying from Montreal to Vancouver and you go into U.S. airspace on, let's say, an Air Canada flight.... You mentioned no-fly lists, but I think it's about passenger manifests. In other words, even though it's a flight from Montreal to Vancouver, the United States government would say because it flies into U.S. airspace they want to have the manifest of the people on that flight.

I'm just curious to explore that in the sense of how you in your job —and it's a difficult one, I acknowledge that—go through the calculus in your own mind when you're weighing up these competing interests.

For example, I'm hoping that as a government we could negotiate out of that, or that we don't have to do it. But if I put my shoes in the position of the U.S. government, I might say to myself of someone who is flying in our airspace and who could take action to commandeer that aircraft—I suppose you could argue that someone could do it if they were flying over Finnish airspace or Canadian airspace as well, but if they are in our airspace—that I might like to just know a little bit about them and run them against my list.

This does present some privacy challenges, I suppose, because this is a within-Canada flight. I'm not necessarily asking you what your views are on it, although I guess you can offer them, but how do you do the weighing in your own mind of these competing interests?

Ms. Jennifer Stoddart: Yes, that's a very good question.

This particular issue is one we've just started to look at. I think the first thing you have to understand clearly, apart from one's reluctance about the practice or the procedure and how it would impact on you or people you know, is what exactly are the rights of different countries and the rules of international aviation that bind the flying of civil aircraft over spaces of countries and so on. That would be the first step to clarify exactly what the issues—

● (1925)

Hon. Roy Cullen: Let's assume for the moment that it's—

The Vice-Chair (Mr. Kevin Sorenson): Let's get the answer to the question. We're way past already.

Hon. Roy Cullen: Okay. I was just going to say, let's assume it meets the international law test, that it would be legal for them to ask for that manifest.

Ms. Jennifer Stoddart: Then I think we would look, if it is legal under Canadian law, at whether there are steps you can take to mitigate the impact on Canadians' privacy rights. Indeed, over the last few years one of the focuses of this office's work has been around the debate on passenger lists, what's called advance passenger information/passenger name record, in order to make sure, if you have to comply with international law and international civil aviation standards, and this is coming up increasingly, that you do it in a way that's the least privacy invasive to people; that people are informed of their rights; that the information that may be collected is not used for other purposes—basically, that we apply fair information principles to those practices.

The Vice-Chair (Mr. Kevin Sorenson): Thank you, Commissioner.

We're on a five-minute round now. I've been fairly lenient on the seven-minute round; some of them were nine minutes. We'll try to keep them...and hopefully everyone will be able to ask every question they want.

Mr. MacKay.

Mr. Peter MacKay: Thank you, Mr. Chair.

Ms. Stoddart, I began my questioning with reference to the issue of accountability and transparency being key to this exercise and this legislation. One of the elements around the debate on national security and anti-terrorism is this necessity, I would call it, for greater oversight and review of the activities of law enforcement security agencies, and I think I read into your recommendations and your comments that you share that view.

In recommendations 8 and 17, again your basic premise is the need to inject more oversight. One of the things this committee implicitly is interested in is a body of parliamentarians from all parties—so a non-partisan body—that would be tasked with this type of oversight, even so far as, in extraordinary circumstances, being privy to operational detail. In the context of your recommendations and your feeling for the need for more security, if you endorse this idea, do you favour having a parliamentary oversight committee as part of this process?

Ms. Jennifer Stoddart: Yes, absolutely, and I think that's one of our key recommendations, and one that I think Parliament could act on.

I personally feel this is essential, because one of the dangers in a democratic society is that we have security and intelligence operations run by experts in the field, who now wield these extraordinary powers and are increasingly divorced from ordinary Canadians, who have to take it on faith that all these powers are necessary. I think that because Parliament or the House represents the elected members of the public, it is extremely important in making a link between ordinary Canadians and what is actually happening within the security and intelligence milieu.

So I think this is a key recommendation, and something that would be an important addition.

Mr. Peter MacKay: Do you feel your office is playing that role to some degree? Do you feel that you've undertaken this function and that it is part of your mandate?

Ms. Jennifer Stoddart: I don't think, honourable member, that we have the scope or the resources. We have many mandates in the public and private sector. I don't think historically.... And certainly under the Privacy Act, which dates from 1983, we're not particularly focused on security and intelligence.

Mr. Peter MacKay: Is it found in the legislation anywhere? Can you read in an interpretation that gives you that mandate?

Ms. Jennifer Stoddart: Certainly we have extensive audit power. We could presumably audit any security agency tomorrow, but there's a very practical question of the type of resources that it would take.

Mr. Peter MacKay: It often is an issue of resources.

Another question on the mandate side is, do you also see yourself involved in the advocacy and promotion of privacy in Canada? Is that something you promote?

Ms. Jennifer Stoddart: Oh yes. That's our specific mandate under our most recent legislation, PIPEDA, and we've asked that it be included in what we hope is a reform of the Privacy Act.

● (1930)

Mr. Peter MacKay: So it's not there now, or not explicitly in the legislation?

Ms. Jennifer Stoddart: It's not explicit, and we don't have a very explicit educational mandate, but de facto we have an educational mandate that we exercise through our website and educational materials and so on. But we would like it to be written in.

Mr. Peter MacKay: On the previous issue, then, with respect to a mandate to include oversight, to some degree, of these security agencies, has the expanded mandate, implicit or otherwise, impacted on your ability to do all of these other things the office was originally set up to do? Tie that into resources, tie that into mandate, and tie that into person power.

Ms. Jennifer Stoddart: Exactly. We don't have the person power, and there is also in our world now the technical or technological power. That's a big part of our job, and we have to gear up on that and hope we have the resources to gear up. It takes a lot of technological expertise to be able to that.

But if I can finish answering the question of the honourable member, I think our role is limited to tracking where information is, how it's handled, and so on. We are not geared to evaluating the quality or the strategic significance of information in a security or intelligence context. That is a role for a committee of parliamentarians, so I don't think there's any way we should stray into that field.

Mr. Peter MacKay: Thank you.

The Vice-Chair (Mr. Kevin Sorenson): Thank you.

Mr. Wappel.

Mr. Tom Wappel: Thank you very much for coming and staying.

I have a whole bunch of questions on a whole variety of topics, but let's just start from where Mr. MacKay left off, because I'm not quite sure I understood your answer.

I believe you agreed with him when you said that you saw your office as an advocate and promoter of privacy rights and, I believe, you called it a different thing.... Was it information? What did you call it?

Ms. Jennifer Stoddart: Protection of personal information?

Mr. Tom Wappel: No. You said something about providing information or disseminating information, or something like that. I guess I'll have to check the blues. I'm sorry, but I should have written it down.

Let me re-ask the question. Do you and your office see yourselves as an advocate and promoter of privacy rights?

Ms. Jennifer Stoddart: Yes, we do.

Mr. Tom Wappel: Okay. And what part of what act gives you that power?

Ms. Jennifer Stoddart: PIPEDA, the Personal Information Protection and Electronic Documents Act, specifically gives us that power.

Mr. Tom Wappel: In what section?

Ms. Jennifer Stoddart: It might be section 23. I'll get our general counsel to look this up.

As I remember, it isn't explicitly named in the Privacy Act, but I'll say that the Office of the Privacy Commissioner of Canada is set up as an ombudsman's office. I would argue implicitly, then, with the ombudsman's model comes a role for education in our system, and that's how it's been interpreted by successive—

Mr. Tom Wappel: Oh, that was the term: education. Don't you think there's a difference between educating the public about their privacy rights and advocating and promoting privacy rights in general? Do you see any difference between those two phrases?

Ms. Jennifer Stoddart: Perhaps stated like that, yes. But in particular context, part of education can be making people aware of how to advocate for their rights and how to promote their rights. Although in a dictionary sense these terms are distinct, in the—

Mr. Tom Wappel: Because in the one case, the *Ottawa Citizen* is advocating and promoting their rights, and in the other case, the commissioner is advocating and promoting the esoteric topic of rights. I see a distinction.

Ms. Jennifer Stoddart: Well, we do different things in different contexts. We come before you here and we talk about the privacy rights of Canadians. We're advocating privacy rights of Canadians.

Mr. Tom Wappel: The only reason I mentioned it is that it has been my observation over many years here—and this is absolutely no reflection on you, it's just in general—that bureaucracies, departments, commissions, and commissioners tend to exponentially increase and try to absorb more and more power and get bigger and bigger. And that's a historical observation of 5,000 years of bureaucracy in every possible context of every possible government. It's just the nature of things. I don't want to get into a big philosophical discussion about it.

But in your opening remarks—let's get this clear—you have a different font size than we do. You mentioned you had written to the minister of the Treasury Board, and then you said you had received an answer. I want you to know that in our copy you have addressed the answer of the minister. So if that's what you're referring to as the missing pages, they're in fact not missing; it's just that your document is longer because it's bigger than ours, which has smaller print. We've figured that out. So we're okay there. You don't need to send us anything.

● (1935)

Ms. Jennifer Stoddart: Okay, thank you. I'm relieved

Mr. Tom Wappel: Back to your opening remarks, your first comment was that the act should be subject, in its entirety, to a five-year recurring sunset clause, which is an interesting thing. I don't see that among your 18 recommendations. I see recommendation 14, which does not say the same thing, the way I read it. So is this now recommendation 19?

Ms. Jennifer Stoddart: Well, if that would help the committee to organize its work, let's make it recommendation 19.

Mr. Tom Wappel: I'm sure you'll agree there's a difference between an automatic sunset clause of legislation every five years and a parliamentary committee that will review it. One is a review process, and I think that's what recommendation 14 says. I could be wrong. Let's have a look: “should be subject to periodic Parliamentary review”. Parliamentary review is what we're doing, but no matter what we do, no matter how long we take, a sunset clause is different, because a sunset clause would expire the legislation unless certain things occurred.

So I guess now you're saying there should be current parliamentary review, an ongoing parliamentary review, and oh, by the way, every five years this act should stop, unless something positive is done. In fact, there's a provision in the act, for some of the sections, for that very thing to happen—section 83-something.

If I might, could I add that, then, as recommendation 19 to your recommendations?

Ms. Jennifer Stoddart: Yes, if that would be helpful, or it might be recommendation 14.1, because it seems to me that it's a technique of periodic review.

Mr. Tom Wappel: Recommendation 14.1, then. Perfect.

The Vice-Chair (Mr. Kevin Sorenson): Very quickly, Mr. Wappel.

Mr. Tom Wappel: I want you to know that of all the government agencies and various ministers that have appeared here, as far as I know, Mr. Chairman, nobody has recommended any changes to the act except you. I find this startling. Everybody who has come here has said there is nothing wrong with it, it's great, it's fine. Today we asked the RCMP, and everything was okay. We asked the minister, and everything was okay. We asked FINTRAC, and everything was okay. We asked CSIS, and everything was okay. Yet you have 18 recommendations

This is fascinating to me. It's neither a negative nor positive comment; it's just interesting to me that it has taken us this much time to get a government agency of some nature to come up with some recommendations that it thinks might improve the bill. Everybody else thinks it's great and wonders why we're wasting our time. I find this fascinating.

The rest of this I'll leave for my next chance.

Thank you.

The Vice-Chair (Mr. Kevin Sorenson): Thank you, Mr. Wappel.

I think you're making reference to the fact that we've been hanging around with the wrong crew maybe.

An hon. member: Oh, oh!

The Vice-Chair (Mr. Kevin Sorenson): Mr. MacKay.

Mr. Peter MacKay: Thank you, Mr. Chair.

One of the facts that you wouldn't be aware of—and Mr. Wappel has referenced a number of other witnesses—is that one of those witnesses before us, the CSE commissioner or chief of the Communications Security Establishment, was very adamant that his office was operating completely within the law and within their mandate. Yet in recommendation seven, I couldn't help but notice that you said that "the National Defence Act should be amended so that the CSE Commissioner is required to ensure" not only that intercepts are authorized by the minister, but also that they are "authorized by the law and consistent with the Canadian Charter or Rights and Freedoms and the Privacy Act". That stood out.

Have you, in fact, had complaints that there were ministerial authorizations not authorized by the law?

Ms. Jennifer Stoddart: No, we haven't. Because of the nature of what's happening there, I don't think people would really know about it, so we can't say this is informed by any complaints. I think this is simply a suggestion to raise the standards for the use of ministerial discretion.

● (1940)

Mr. Peter MacKay: All right.

The other question I have is a very straightforward one about recommendation three, where you talk about the Criminal Code's time limits, that 60 days' authorization and up to one year for notification should be required, and that the exceptions in the Anti-terrorism Act allowing for warrants to be extended for up to three years without authorization should be repealed. I'm curious as to why you believe that discretionary extension power should be withdrawn.

I've worked as a crown prosecutor and I know that even under the Criminal Code, when people are fleeing the jurisdiction and are at large, oftentimes off the continent.... When we're dealing with international terrorists, I would suggest that is very much the norm, if there is such a thing as a norm when it comes to terrorists fleeing.

So I'm just curious as to your rationale for favouring the withdrawal of the ability to authorize that type of extension.

Ms. Jennifer Stoddart: Clearly, we're not involved with these kind of warrants, so we don't have the experience that you may have with them, but we proceed from the position of principle, that we should conform to the common line of existing legal standards in Canada as much as possible. Straying beyond that line into this type of very stringent security legislation is an important step.

Perhaps you've heard other witnesses who have given you this information, but in the material we reviewed, we did not see this kind of extraordinary time period being consistently used and thus still needed.

Mr. Peter MacKay: Is the concern with the process of the extension or just with the concept of extending it beyond the normal period without further evidence, or the necessity to reappear before a judge?

Ms. Jennifer Stoddart: Our concern here is with the extent of the time period without the necessity of going back. We presume that one can go back and ask for an extension, and as I said, we didn't come across a body of evidence that said this has been a key factor in lessening the terrorist risk in the last five years in Canada. So we take this as a position of principle.

Mr. Peter MacKay: Can I ask you a general question by way of background? In your experience in this role, have you had occasion to look outside the Canadian experience? Have you looked at other jurisdictions? I'm talking now in the context of the anti-terrorism legislation. Have you examined the practices and procedures as they relate to privacy in other jurisdictions, in coming to some of the conclusions and recommendations you've given us?

Ms. Jennifer Stoddart: No, not systematically. We've haven't been able to do that, which would have been ideal. Perhaps sometimes in looking at one measure, we would have read something about another country. But unfortunately, no, we haven't been able to do that, which would have been ideal.

Mr. Peter MacKay: Thank you, Commissioner.

The Vice-Chair (Mr. Kevin Sorenson): Mr. Wappel.

Mr. Tom Wappel: Thank you.

Let's carry on with recommendation three.

Before I ask my question, I've been desperately trying to find the relevant section. Can Ms. Kosseim help me find the section dealing with warrants of up to a year and up to three years?

Mrs. Patricia Kosseim (General Counsel, Office of the Privacy Commissioner of Canada): It's on page 44, which amends paragraph 196(5)(c) of the Criminal Code.

I go by page numbers, because they are a bit easier to use with this legislation, so if you look at page 44, it's the bottom provision.

Mr. Tom Wappel: My question is whether the word "authorization" is the correct word, or is it the word "notification" in your recommendation? I'm asking the question, should it not be "without notification"? Surely the thing is authorized in some manner, either by the statute or the minister, but the person isn't notified of the fact. I'm wondering if there's an incorrect word usage there.

If you don't have an answer, that's fine, but maybe you could just look into it. If it turns out that's the case, just let us know. It's a small point, but this is such a complicated thing, sometimes if you miss a word the whole meaning goes the other way.

Am I on the right track there? I think it should be "notification". You'll take a look at that.

● (1945)

Ms. Jennifer Stoddart: Okay, we can get back to you.

Mr. Tom Wappel: We understand what you mean, but let's use the correct terminology.

If I might say so, I thought your idea of a security-cleared special advocate is an interesting one. Certainly I think there should be periodic parliamentary review; I think that's a good idea. And I think that a sunset clause forces periodic parliamentary review, which is something that should be considered—that's just on my part. I think these are good ideas, worthy of further consideration.

I'm a little unsure about recommendation six. How do you limit the information that CSE can obtain?

Ms. Jennifer Stoddart: I must say, I don't know from my personal knowledge. I think our suggestion there is simply to change the wording to go to a tighter concept of limits to the concrete obtainment of material. I believe the commissioner is responsible for the oversight of the Communications Security Establishment and would be the only one to look at how that's enforced. He presumably does that according to the law governing the Communications Security Establishment.

Mr. Tom Wappel: You've got to obtain the information before you can determine whether or not it's relevant, whether or not the information you obtained is within the jurisdiction or the law, or is permissible, or whatever the case may be. I take it that what you're meaning is that once the information is obtained, there should be tighter limits on its use or availability. I find it difficult how you would legislate preventing CSE from obtaining certain information.

Ms. Jennifer Stoddart: We're referring to the paragraph that talks about satisfactory measures, that the minister can issue an authorization if he's satisfied that, among other things, “satisfactory measures are in place”. The paragraph reads: “satisfactory measures are in place to ensure that only information that is essential to identify, isolate or prevent harm to Government of Canada computer systems or networks will be used or retained”.

We think it's a more stringent standard to simply place a limit on the obtainment of information—but this is in the intelligence context.

Mr. Tom Wappel: Yes, but how can one do that? How does one turn off the tap? I mean, information pours in. Surely the criterion is, what do you do with that information?

Ms. Jennifer Stoddart: Well, I think it would suggest there's a test, perhaps a reasonable person test or a reasonable expectation that the information this intelligence agency obtains is only what is really necessary to do that part of protecting Canadian computer systems.

What we're trying to do is to say, instead of sweeping everything in your path in the worthwhile objective of protecting Canada's computer systems, could we have a more stringent test, to just try to obtain what is necessary for that task? That is the essence of our suggestion.

Mr. Tom Wappel: All right.

If might ask a final question in this round, do you, as the Privacy Commissioner, have any concrete case brought before you of anyone's privacy rights being abused by this legislation?

Ms. Jennifer Stoddart: Not that I'm aware of.

Mr. Tom Wappel: Thank you.

The Vice-Chair (Mr. Kevin Sorenson): Monsieur Ménard.

[*Translation*]

Mr. Serge Ménard: I agree with many of Mr. Wappel's comments. I don't know if I needed to share that with you, as you're basically here to answer our queries.

There's no question, for instance, that the systematic review of the Act every five years is justified. It's also true that yours is the first organization recommending substantive amendments to the legislation, although I believe that's also your role in government, a role that you play very well, I might add.

I would have broached the last question somewhat differently, but I will put the question to you nonetheless. Have new anti-terrorism laws adopted recently affected your operations? Have you received more complaints from citizens? Has the only impact noted been the decision by your Office to examine the Act and make recommendations to lawmakers, or have these laws prompted some concerns and curiosity on your part as to whether other countries that have passed similar laws harbour similar concerns?

When highly traumatic events like these occur, lawmakers assume a certain role, otherwise they feel that their constituents... Since their only role is to legislate, then that's what they do, even if the problem cannot necessarily be solved by enacting laws. The key in fact may lie in better organization and in the allocation of additional resources to law enforcement agencies and specifically in this case, to intelligence agencies.

I for one believe that laws are not the key to fighting terrorism, because we're already talking about something that is illegal in many regards. The key to combating terrorism lies in intelligence gathering and sharing operations.

Therefore, I'm hearing you say that ordinary citizens have not voiced the same concerns as the intelligentsia who are worried about whether or not laws are consistent.

● (1950)

Ms. Jennifer Stoddart: Mr. Chairman, one of the problems with the legislation under review by the committee is that ordinary citizens don't really know if they can in fact file a complaint with our Office over the enforcement of the act's provisions.

Mr. Serge Ménard: That's true.

Ms. Jennifer Stoddart: This is of great concern to us. Admittedly, Canadians are not lining up to complain that their rights are being violated because of these new measures. If there have been complaints, they've being raised in other forums.

However, we've observed a number of indirect consequences. Over the past five years, the operations of our Office have really been focused on the ramifications of the Anti-terrorism Act, and in particular, the increased incidence of information-sharing among the world's allied nations. You spoke of flights over the United States, and that's one example. Sharing passenger manifests is another. The public is quite concerned and anxious about this situation. The impact on our Office has been marked.

As I believe I mentioned in my opening presentation, we recently conducted a poll. We found that increasingly, Canadians have very clear opinions about informational privacy issues and concerns about how this information is disseminated. Specifically, they are concerned about the fact that information could be shared with a foreign entity and about the lack of minimal controls, whether in a civil or national security context. All of these concerns have indirectly led to an increase in our workload, so to speak.

Mr. Serge Ménard: Have you shared the poll results with the committee? I seem to recall having seen them.

Ms. Jennifer Stoddart: I mentioned the poll in my opening statement.

Mr. Serge Ménard: I know, but I'm talking about the poll results.

Ms. Jennifer Stoddart: Would you like us to send you the poll results?

Mr. Serge Ménard: Have you already done that?

● (1955)

Ms. Jennifer Stoddart: No.

Mr. Serge Ménard: I seem to recall reading about them, but I can't remember the exact context.

In recommendation 17, you express support for the proposed creation of a National Security Committee of Parliamentarians. Do you have an opinion as to the composition of this committee?

Ms. Jennifer Stoddart: No. Quite frankly, that question should be left to the experts. I have no definitive opinion on the subject. However, I do feel that the committee should have all the powers and resources it needs to carry out its mandate properly.

Mr. Serge Ménard: Do you feel the Committee should reflect the make-up of the House?

Ms. Jennifer Stoddart: Technically, it should. Let me phrase the question differently. Is there some reason why the committee should not reflect the composition of the House of Commons, since we are talking here about giving members of the public, through you, some insight into how these powerful intelligence and security agencies operate?

Mr. Serge Ménard: Well, one reason I can think of...

[*English*]

The Vice-Chair (Mr. Kevin Sorenson): We're almost at seven minutes, so we'll go to Mr. Wappel.

Mr. Tom Wappel: Thank you, Mr. Chairman.

If Mr. Comartin has some questions, I'd be prepared cede this round to him.

The Vice-Chair (Mr. Kevin Sorenson): Can we back up and let Mr. Ménard just finish his last little—

Mr. Tom Wappel: Yes, that's fine. I have questions, but I don't want him just sitting there waiting—

The Vice-Chair (Mr. Kevin Sorenson): We may even stretch this past 8 o'clock a little bit. I want everyone to get a chance.

Did you have another question, Monsieur Ménard?

[*Translation*]

Mr. Serge Ménard: Yes. To justify the fact that the committee may not fully reflect the make-up of the House, we're hearing the argument that in the event it actually did, those who would want to destroy the country would have an opportunity to make representations. The feeling is that these individuals should not under any circumstances be given access to confidential information.

Ms. Jennifer Stoddart: I think parliamentarians are the ones who should be debating that question and deciding if this would hinder the smooth operation of the national security committee.

Mr. Serge Ménard: We checked elsewhere and got some answers.

The Vice-Chair (Mr. Kevin Sorenson): Thank you.

Mr. Comartin.

[*English*]

Mr. Joe Comartin: It's along the same lines, Madam Commissioner. Mr. MacKay, Mr. Ménard, and I, and a half dozen other parliamentarians spent most of last summer and early fall working on a report. Have you seen that report?

Ms. Jennifer Stoddart: Yes.

Mr. Joe Comartin: My question, then, is to focus on the mandate of the committee. Mr. MacKay has already made some reference about parliamentarians having the jurisdiction, when warranted, to actually be able to have access to operational information. In this light, I'd like your comments with regards to that. If in fact you were able to do that, get the committee set up....

Perhaps you should know, the minister has indicated that the legislation, I think, is finished and is pending to come before the House, hopefully before we adjourn for the summer. I have no idea what the mandate is going to be, because this has been a major bone of contention. But with regards to it, if the parliamentary oversight committee had the authority to actually even look into operational incidents, would we provide additional protection to the privacy rights of Canadians generally?

Ms. Jennifer Stoddart: I think so, yes. I think it's a big challenge to know who can look meaningfully upon the work of these very powerful, very important agencies. I would think that the appropriately constituted parliamentary committee, with the appropriate powers, would be the best solution one could devise in a democracy. But there are many variations on this. I know it's a subject of expertise on its own. I don't pretend to.... You've looked at it at length, and it's hard for me to go further than that, but certainly in terms of principle, I think it would be very effective.

Mr. Joe Comartin: Looking at alternatives to that parliamentary committee, you've indicated that your office, both because of resources and mandate, given the nature of the subject we're dealing with—that of an intelligence agency—is literally not able to do it. Is there any other logical agency now existing, or one that could be expanded, within the federal government to do that type of oversight that would protect privacy and the democracy?

Ms. Jennifer Stoddart: You have one major agency, the Security Intelligence Review Committee, and then you have the commissioner for the Communications Security Establishment. I suppose you could look at expanded power issues.

I believe you also have a gap, and perhaps that would be a direction in which to move. The RCMP does not have consistent oversight. They have a complaints committee. As I tried to say, I think there's an issue with complaints only. You have to complain about problems you know about. In today's world of electronic information, you don't know. So I would think you have to look at what agencies there are, what intelligence agencies or police agencies do not have any oversight, and move to fill the gaps.

● (2000)

Mr. Joe Comartin: Have you done any analysis of the other agencies, like SIRC or the RCMP Complaints Commission, in terms of what they do? Is it broad enough to protect privacy rights, even in those limited agencies that they are responsible for?

Ms. Jennifer Stoddart: I don't think they have a particular mandate to protect privacy rights. We have a particular mandate to do audits to protect privacy rights, but obviously gathering intelligence is almost anonymous.

Mr. Joe Comartin: I guess I'm really asking, do you see any of them protecting privacy rights as a byproduct of what their main mandate is?

Ms. Jennifer Stoddart: Yes. Clearly, a good part of their job would be to make sure the information is circulated or used according to the protocols and the laws that we give ourselves, so in that case it's very close to the work of the Privacy Commissioner. But they would be specialized agencies. They would have knowledgeable people on them, and they would have particular clearances and so on. So I don't think they would at all be duplicating the work of the Privacy Commissioner. I think there's a parallel role for us in things that are perhaps further from intelligence but closer to ordinary operations, like what we're doing at the Canada Border Services Agency, that will not go specifically into the details of intelligence work.

The Vice-Chair (Mr. Kevin Sorenson): Thank you.

Mr. Wappel, do you have another question? If you have another question, let me know and we'll sneak it in.

Mr. Tom Wappel: I just have a couple of comments.

In recommendation nine, you're saying that "A more proportionate alternative is to allow the judge to hold proceedings in camera when necessary to protect national security". How does the judge know when it's necessary, unless you hold the hearing in camera and listen to the evidence and then determine that it's necessary?

Ms. Jennifer Stoddart: I would think that the judges doing the job would have a knowledge of their file and would consult with the attorneys and would see—if they can't see in advance when the proceedings develop—at what point it would be necessary to go in camera. I would think the procedure would be somewhat akin to what happens in criminal trials or in access to information and privacy hearings, where proceedings are in camera at some point. Or they're *ex parte*, so perhaps it's not different from an *ex parte* proceeding, in that at some point, it's clear from the trend of the evidence that it should go either *ex parte* or in camera. I think that's part of a judge's job.

Mr. Tom Wappel: But we're not dealing with whether evidence would be excluded, but with very secret, secure national security matters, which should presumably be made available to the least number of people the least number of times. That's my difficulty.

Anyway, you've answered my question, so that's all.

Ms. Jennifer Stoddart: I think we're basically saying that we can have confidence in our judiciary to know at what point the hearings have to go in camera.

Mr. Tom Wappel: I don't have that confidence in our judiciary, as a blanket statement. But that's just me.

Some hon. members: Oh, oh!

Ms. Jennifer Stoddart: Presumably, it would be raised by the Crown too, suggesting to the judge that it should be in camera.

Mr. Tom Wappel: Okay.

On recommendation one, could you help us as to how this can be done? How can you conduct an empirical assessment of extraordinary powers that haven't been used?

● (2005)

Ms. Jennifer Stoddart: Well, we thought this was perhaps an exercise that could be taken up by the committee of parliamentarians.

Mr. Tom Wappel: Because it would have to be in secret, obviously, and there would have to be a complete examination.

Ms. Jennifer Stoddart: That's right; it would have to be a special committee with top secret security clearance, with the power to ask the agencies to appear before it and to look at the facts and at the powers. If their powers haven't been used and you look at the facts, well, you know....

Mr. Tom Wappel: Let's assume that is done with top secret clearance. I guess the only thing the review could say is, yes, we think it's okay, or, no, we don't.

Ms. Jennifer Stoddart: Well, it depends on whether or not it's all top secret.

But I think this would be a lot better, and the public would have confidence, if there are representatives of Parliament who have looked at this information for them and tell them, yes or no, this where we should go. I think the public understands. We understand that these are security matters; we're not saying make them public, but we're just saying we want to know that—

Mr. Tom Wappel: So you'd say that one of the functions of the committee mentioned in recommendation 17 would be that of recommendation one?

Ms. Jennifer Stoddart: Yes, it could be to do recommendation one. There may be other ways to do it; presumably, the government of the day could do it itself.

Mr. Tom Wappel: Yes, but who's going to trust the government of the day? Surely the whole idea is that the government of the day is going to want every power it can have, or arguably it will—let's put it that way. So that's the whole idea.

Ms. Jennifer Stoddart: That's why we think a national security committee of parliamentarians is a worthwhile idea.

Mr. Tom Wappel: Perfect.

Thank you very much, Commissioner.

That's it.

The Vice-Chair (Mr. Kevin Sorenson): Thank you.

Mr. MacKay.

Mr. Peter MacKay: I love your optimism; I do hope the public have growing confidence in parliamentarians.

Voices: Oh, oh!

Mr. Peter MacKay: In recommendation 10, Commissioner, you suggest that subsection 38(13) should be repealed. Basically, your assertion is that "it is superfluous to allow the executive to trump an adjudicative order for disclosure". That's a very interesting way of putting it.

I'm fascinated that you essentially say this process—in which it is quite extraordinary for the Attorney General to personally issue a certificate to prohibit disclosure of information to protect national security or defence—is superfluous. You go on to say that this section already empowers a judge to make a decision if disclosure of information would be injurious to international relations.

I'd just like to give you the opportunity to expand on that a little bit. Are you further asserting, and this is my question, that the Privacy Commissioner should be involved in that decision as well, or should play some role in it?

Ms. Jennifer Stoddart: No, I don't think so.

Mr. Peter MacKay: No? Okay.

Ms. Jennifer Stoddart: Maybe I'll just give you the general gist of our remarks, and then Patricia Kosseim could give you some more technical remarks.

This goes to my answer to the previous honourable member's questions about restoring some of the pre-existing powers to our judiciary to review orders made by the executive in terms of balancing the roles of the different branches of government, in terms of making sure the law is applied correctly and that we come up to charter standards. The judiciary are a type of watchdog. One of their roles in a democracy, as you know, is to see that we follow these basic values we have.

So we strongly question why our judiciary has been set aside from its normal role of revising the application of the law. I believe there is one decision that's come out—the Ribich decision of the Federal Court of Appeal—that seems to give very extensive tests for national security interests. I think we do have a capable judiciary in Canada. I am puzzled as to why we have.... We have several levels of judiciary.

Mr. Peter MacKay: Just before we leave that point, are you aware there are some federal judges who have publicly expressed reservations about being empowered to do just that?

Ms. Jennifer Stoddart: I have perhaps not read their remarks directly. They have reservations about making decisions in national security cases on the evidence and on the application of the law?

Mr. Peter MacKay: Yes, in certain instances where they have the final say on processes such as the investigative hearings, there is a certain ill ease, I guess I would put it, expressed by some, not all, in the judiciary that in some cases, when it involves international terrorism—and I think this is a very humbling remark for a judge to make—they may not be qualified.

● (2010)

Ms. Jennifer Stoddart: I understand that. I think the heart of the decision goes to whether the person is a security risk or to the application of the law. And clearly, one doesn't want to over-expand the role of the judiciary. Its role is not to make decisions in the place of elected officials and the government.

I think the issue is whether there is a review of the application of the criteria. That is usually the standard. So we're talking about whether the criteria are being correctly applied and not judges making the substantive decision in the place of the government. That would be my understanding of how it should work.

Mr. Peter MacKay: Okay.

Did you want to add anything?

Mrs. Patricia Kosseim: I would only say that the evaluation criteria under section 38.06 seems to be fully adequate in terms of providing the judiciary with exactly that opportunity to assess all the criteria to determine whether or not the law had been appropriately applied. That was the Court of Appeal decision in Ribich, which expounded at length on the court's role under section 38.06, and that we think is sufficient in and of itself. In that sense, we thought section 38.13 was superfluous.

Mr. Peter MacKay: Okay.

Finally, the evidence that's been heard already and in recent days before the Maher Arar inquiry, some of which touched upon this concept of consular information being shared with law enforcement or security intelligence agencies, is part of the broader concern about increased use of what is called "data matching" or "data mining". You're familiar with those terms as an investigative technique.

I'm wondering if you can tell us your impression of those techniques, whether this is something your office monitors, and whether there has been an increased use of these types of techniques that you're aware of, post 9/11.

Ms. Jennifer Stoddart: Yes, this is something we're very interested in.

May I ask the assistant commissioner to perhaps give you some more information, because he is particularly interested in this phenomenon and we have—

Mr. Raymond D'Aoust: Actually, Treasury Board had adopted a policy back in 1989 requiring department heads to report on and notify us of data matches. It's our view that this policy is largely... [*Technical difficulty—Editor*]. The definition proposed in our policy is very clear. We've been having discussions with Treasury Board to broaden that definition to capture not just back-end type of data matching—*ergo* to determine eligibility or fraud, and so on—but also data verification, and also for non-administrative purposes as well, like research and so on. So we're looking at that, to have a better policy.

Just last year, we only had 10 notifications of data matches. We believe that was clearly an underestimation, if you will, of the data matches that are actually occurring in federal operations, if you like. So we're looking at that.

Mr. Peter MacKay: Thank you.

That's all I have.

The Vice-Chair (Mr. Kevin Sorenson): Thank you for coming. Certainly, I think each one of us would say that it's been very worthwhile having you here tonight.

Thanks again for coming.

Ms. Jennifer Stoddart: Thank you very much.

The Vice-Chair (Mr. Kevin Sorenson): The other thing I should mention is that although we figured out the font size and the difference in pagination, you did make a number of references to the poll that your office had undertaken. If we could get a copy of that survey or poll, the questions asked and the results, it might be very beneficial to us.

Thanks again.

Mr. Comartin.

● (2015)

Mr. Joe Comartin: I'll say thank you also.

I just want to deal with a business issue. We must have at least a 15-minute to a half-hour meeting to deal with future business.

The Vice-Chair (Mr. Kevin Sorenson): Can we adjourn, and then we'll just talk about this off the record? Or do you want it on the record?

Mr. Joe Comartin: I just wanted this on the record.

The Vice-Chair (Mr. Kevin Sorenson): Okay.

Mr. Joe Comartin: We have to schedule something. I've got a lot of witnesses on the question of certificates who are waiting, and I can't give them any direction. And some of it may require some travel, too, Mr. Chair.

The Vice-Chair (Mr. Kevin Sorenson): Mr. Zed isn't here today because of a health issue, and I don't know what the proper protocol is. But I would maybe just relay to him via the clerk—as I see that Mr. Zed's staffer has gone—that this is a very important thing. If we're going to bring witnesses in, we have to be courteous to them and give them time to be prepared and to know what timeframe we're on here.

We'll leave that with the clerk. I will talk to Mr. Zed when I see him. I think we'll all pass on the sense of urgency we have as a committee.

Mr. Joe Comartin: Thank you, Mr. Chair.

The Vice-Chair (Mr. Kevin Sorenson): We adjourn.

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 Parliamentary Internet Parlementaire at the following address:
Aussi disponible sur le réseau électronique « Parliamentary Internet Parlementaire » à l'adresse suivante :
http://www.parl.gc.ca
