



House of Commons  
CANADA

# Standing Committee on Public Safety and National Security

---

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

---

EVIDENCE

**Thursday, May 7, 2009**

—  
**Chair**

**Mr. Garry Breitkreuz**

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

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

## Standing Committee on Public Safety and National Security

Thursday, May 7, 2009

• (0905)

[English]

**The Chair (Mr. Garry Breitkreuz (Yorkton—Melville, CPC)):** I call this meeting to order.

This is the Standing Committee on Public Safety and National Security, meeting number 20. We are continuing our review of the Iacobucci and O'Connor inquiry reports.

We would like to welcome our witnesses this morning. We have the Office of the Privacy Commissioner, represented by Ms. Jennifer Stoddart, the Privacy Commissioner. She will introduce the people she has with her. As an individual we have Mr. Paul Cavalluzzo.

I understand you have agreed that Mr. Cavalluzzo will go first.

We usually allow approximately 10 minutes for an opening statement. After you've made your opening statement, we'll go to questions and comments.

Without any further ado, we'll go ahead.

**Mr. Paul Cavalluzzo (Counsel, As an Individual):** Thank you.

Mr. Chair and honourable members, thank you for giving me the opportunity of discussing with you the Arar report, which was presented by Justice O'Connor in September 2006, and part two was delivered in December 2006.

In that regard I acted as his commission counsel in the Arar inquiry, which was conducted over a period of two and a half years. In the limited time I have today in my presentation, I want to focus on the recommendations that were made by Justice O'Connor in parts one and two.

Now I'll give a little background.

As you know, Maher Arar is a Canadian citizen who was stopped at the Kennedy Airport in New York City in September 2002, where he was flying through on his way back to Montreal. He was detained by American officials for 12 days and was subsequently removed to Syria, which is the country of his birth. He was interrogated, tortured, and held in inhumane conditions in Syria for close to one year. On October 5, 2003, he was released and returned to Canada.

To this time, he has never been charged with any offence by Canadians, Americans, or the Syrians. In January 2004 the federal government called a public inquiry because of the political pressure that had been building up in respect of the role of Canadian officials regarding the treatment of Mr. Arar in the United States and Syria.

The public inquiry had two parts. Part one was the factual inquiry, wherein Justice O'Connor looked at what happened and reported on the role of Canadian officials in respect of Mr. Arar's treatment. Part two was the policy review, wherein he was called upon to recommend an independent arm's-length review mechanism for the RCMP in respect of its national security activities.

Now, as far as part one is concerned, the what, why, where, and how, just focusing on the main conclusions, an important part of part one was the information sharing that was conducted by Canadian authorities and in particular by the RCMP. After reviewing all of the evidence, Commissioner O'Connor concluded that the RCMP provided American authorities with information that was inaccurate, unreliable, misleading, and that certainly viewed Mr. Arar in a very negative sense. You must contemplate the context of this. This is a year after 9/11, where the American authorities obviously—as was put by one witness—had a great deal of adrenalin as far as alleged terrorists were concerned.

It was also found that the front-line investigators gave the American authorities, the FBI, information on Mr. Arar that was misleading while he was detained in the United States and while the Americans were interrogating him.

Now, as far as his stay in the United States is concerned, there was no evidence that Canadian officials played any role in the decision of the American authorities to detain Mr. Arar. However, the evidence was clear that American authorities relied upon misleading information that was given to them by the RCMP and that no doubt played a role in his detention by the Americans.

As I said before, after about 12 days they removed Mr. Arar to Syria. Even though they had the option of sending him 200 miles to the border outside of Montreal, they preferred to send him 3,000 miles to Syria because of their view that they didn't want Mr. Arar walking on the streets of Canada.

In Syria, as I said before, it was found that Mr. Arar was tortured and was kept in inhumane conditions for close to a year, and unfortunately, even though Canadian officials, consular officials, had access to Mr. Arar on eight occasions during that time, it was not recognized that he was being tortured at that time because of the manner in which the interviews occurred. Syrian officials were present during the interviews, and unfortunately because of lack of training they did not recognize that he was being tortured.

● (0910)

Upon his return to Canada in October 2003, unfortunately, a lot of information was put out about Mr. Arar that was misleading, that violated national security principles because it was confidential information, and it was made to look as if Mr. Arar was somewhat dangerous and somewhat of a terrorist. Unfortunately, that leaked information has never been reviewed in terms of a criminal prosecution. To this day nothing has happened.

As far as the recommendations of part one are concerned, Justice O'Connor made 23 recommendations. I'll focus on the most important ones.

The first one is on information sharing. Obviously Canada must continue to share information with our foreign partners, but he said that surely we have to screen such information for relevance, reliability, accuracy, and to ensure it complies with our privacy laws.

He also said the RCMP individuals or investigators who are involved in national security must be better trained. They might be great police officers, but that does not mean they're competent to conduct a national security investigation.

He also stated that the RCMP should never provide information to a country with a poor human rights record if the information will cause or contribute in any way to the torture or inhumane treatment of a Canadian held abroad. In other words, Canadians should not be complicit in torture.

The other point he makes in terms of torture is that if we are going to accept information from a country with a poor human rights record, we have to look at the political and the human rights implications of that; and if we are going to accept such information, we had better ensure and assess its reliability, because by definition, such information is usually very unreliable.

Moving to part two of the mandate of the Arar inquiry, which was to make policy recommendations concerning a review mechanism for the RCMP, Justice O'Connor concluded that the existing mechanism for review of the RCMP activities is totally inadequate, for a number of reasons.

Over time, the amount of information sharing the RCMP does has increased immensely. The RCMP now has increased police powers, particularly in the area of national security. A number of practices, such as integrated policing along with other partners, require a more effective review mechanism.

He said that because of the secret nature of national security activities or investigations, it's difficult to monitor that by a complaints-based approach, because people, Canadian citizens, really don't know, for the most part, whether these activities are violating policies and the law and so on.

As a result of that, he recommended that the new review mechanism have the authority to initiate a review of RCMP activities in the national security area on its own. This would be very similar to the power that currently exists with respect to the security intelligence review committee with respect to CSIS operations.

Once again, this kind of power is necessary because these national security investigations are beyond judicial scrutiny, for the most part.

The other important enhancement in terms of a review mechanism that he recommended was that the new review body should be given broad investigatory powers, similar to the powers of a public inquiry. He reviewed the interrelationship between the present CPC and the RCMP and found that it was ineffective because of the limited access to RCMP information the CPC had.

He recommends that this new body have the authority to determine what information it needs to effectively fulfill its mandate. This would involve the power to subpoena, the power to compel testimony, and so on.

● (0915)

The new body, which he called the Independent Complaints and National Security Review Agency for the RCMP—ICRA is the acronym, I guess—would have jurisdiction to review all of the RCMP's activities, not only its national security activities. He said that it's a judgment call, but it's better to have one body reviewing all of the activities of the RCMP, because we need a body that is expert in police work and law enforcement, and so on, and there may be jurisdictional problems if you created separate bodies to review its national security activities and its other activities.

Because of the highly integrated nature of most national security investigations—and the Arar inquiry was a good example of that; we had to review the activity of the RCMP, of CSIS, of the CBSA and so on—he said that other agencies that are involved in national security should be subject to review as well, such as the CBSA, DFAIT, and so on.

Finally—I see my time is running out—he recommended the creation of an overall committee, an independent committee that would be composed of the chair of the new RCMP body, SIRC, the CSIS body, the CSE commissioner, and an independent person, which would review all of the national security review that is done by these bodies, as well as being the place where a citizen would go to file a complaint. Any national security complaint would be filed with this new committee, which would determine which of the three bodies should be involved in its review and also make recommendations concerning national security review policy in the future to the government.

I could go on, but I think it's better to leave more matters for questions.

In conclusion, I would suggest that if we do ever get this kind of effective mechanism for a review of national security activities, there will no longer be a need for these expensive public inquiries and ad hoc inquiries that we have had over the last five years. It's going to be a restructured body, not a completely new bureaucracy, and in our view it'll be effective, efficient, and most importantly, will respect our human rights.

Thank you.

● (0920)

**The Chair:** Good, thank you very much.

We'll now turn it over to Ms. Stoddart. You can introduce your colleagues and make your opening statement. Go ahead.

**Ms. Jennifer Stoddart (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada):** Thank you very much, Mr. Chairman, honourable members.

I'm here as the Privacy Commissioner of Canada, and the relevance to the topic we're discussing today is that under the Privacy Act my organization has the authority to take complaints, to investigate, and to audit the personal information practices of more than 250 agencies and departments, including the RCMP, CSIS, and other national security agencies, such as FINTRAC.

Accompanying me today is Chantal Bernier, who is assistant commissioner for the Privacy Act. Madame Bernier was formerly assistant deputy minister in the Department of Public Safety and Emergency Preparedness. And with me as well is senior adviser Mr. Carman Baggaley, who accompanied me when I appeared before the inquiries of Mr. Justice O'Connor and Mr. Justice Major.

I believe all the honourable members have two documents that my office provided to you last week. The first piece is an overview, a background, of national security and surveillance laws passed in several countries since 2001, and it shows how much the social and political terrain has shifted dramatically after 9/11.

I'd like to talk a bit about how privacy laws apply to national security agencies.

In the various cases you were reviewing, this application is all too clear. The men who became the subjects of the inquiries that you were studying, as we just heard, suffered terribly, but as well as all the other harms they endured, the first violation was to their privacy.

To begin with, as Mr. Cavalluzzo has quoted, Justice O'Connor noted that inaccurate and misleading intelligence about them was compiled. That means their personal information, in terms of the Privacy Act, was shared inappropriately. Finally, this information was used to justify their detention, deportation, and subsequent torture.

[Translation]

Privacy rights under Canadian law are not simply about who is allowed to collect information. Privacy laws also set out who is accountable for protecting that information, ensuring it is accurate and limiting its disclosure to third parties. The findings of the O'Connor and Iacobucci reports call into question the practices of Canadian security agencies in all these areas. Both reports underscore how critical it is for officials in these departments to properly manage the collection, validation, sharing and careful review of the exchange of personal information.

[English]

Commissioner Iacobucci concluded in his inquiry that inaccurate information was collected on the individuals in question, that inaccurate information was shared with other states, and that safeguards for these files were not properly observed. Misleading, inaccurate, or out-of-date information was kept on file and shared too broadly, with few or no caveats on the use of that intelligence.

Privacy practices in government must be better defined, and sensitive information must be protected. This has never been more urgent than in light of the national security challenges we face. To address this question, the second piece that we have provided to this

committee presents our views on how oversight, privacy practices, and data protection in government could be improved.

[Translation]

While I have several suggestions for your consideration, if I can leave you with one over-arching message, it would be this—in an era of networked intelligence and surveillance, Canada needs a networked approach to oversight and review. Proper oversight and accountability for national security provide a vital check for Canadians' privacy rights.

[English]

In our recent history, rights and security are often pitted one against another. Margaret Bloodworth, who was Canada's former national security adviser, noted this tension just prior to her recent retirement. She said that safeguarding the privacy rights of citizens while also securing their physical security is not simply a question for the Canadian intelligence community, it is *the* question. It is the question, the single greatest issue that they must confront. I'd also add that security and privacy are not, as we often say, mutually exclusive. We need not, nor should we not in Canada, trade one for the other.

● (0925)

[Translation]

As you have heard from other expert witnesses, a fundamental question for national security in the 21<sup>st</sup> century is data governance. In a fully wired, networked world, how does any organization exercise quality control and oversight? Given the complexity of inter-agency, inter-jurisdictional, international, inter-sector intelligence operations—who can exercise that level of global review?

[English]

A recent report from the Office of the Auditor General in March 2009 on intelligence and information sharing stressed this point, that review bodies “must look beyond individual agencies to reflect the integrated nature of national security activities”. These are the main points that I hoped to raise in our submission.

Now I'll just take you quickly through the recommendations. There are seven of them.

First of all, we recommend adopting an integrated approach to security review that allows for more coordination and more cooperation on investigations and reports across the system. This is the network approach recommended by Justice O'Connor. In my experience and in the experience of my office, this has worked to great effect. We do joint investigations with provincial privacy commissioners' offices. We do collaborative reporting with the Office of the Auditor General, for example. All of the review community, in my opinion, could benefit from similar powers.

Second, I think we have to address the privacy practices within security agencies. The approach of departments and agencies to information sharing and data management has to change. Without proper attention to internal controls, new layers of oversight will not address front-line problems. Enhanced training around the theory and the practice of privacy, fair information practices, and data protection could affect great change here.

Third, appoint chief privacy officers across the government, but in particular for departments and agencies where collection of sensitive personal information is widely required by their mandate.

Fourth, provide the Commission for Public Complaints Against the RCMP with the resources and legal authority required to exercise more meaningful review. I believe Mr. Cavalluzzo has spoken quite completely to this question.

Fifth, request that the Treasury Board and ministers issue new policy requirements for departments and agencies on privacy. Robust information-sharing agreements through privacy impact assessments, well-developed privacy directions, and guidance must become part of how these organizations operate. We cannot have the informal, unstructured, and basically ungrounded sharing of information anymore.

[*Translation*]

Six, reform—as I have said before several other committees of the House of Commons—the Privacy Act, which dates back to 1983. In light of all that we have learned, I believe government departments must be held to a higher standard of privacy protection, information handling and data protection. I have recently put forward 10 “quick fixes” for government’s consideration which could tighten controls on international information sharing, require departments to test the necessity of the information they collect and allow the Federal Court a wider role in reviewing violations of the act.

[*English*]

Seventh and finally, we urge Parliament to increase the resources and involvement of this House committee and its counterpart in the Senate. These bodies can provide active oversight of national security agencies and their operations. By pooling expertise, coordinating reviews, and sharing information, existing mechanisms for parliamentary review could be augmented.

Briefly, Mr. Chairman, I’d like to leave you with a few final thoughts.

While Canada’s system of review and oversight functioned throughout the 1980s and 1990s, the stresses on the system after 9/11 have become tragically apparent. This needs to be addressed. When networks of intelligence sharing are global, oversight cannot remain rigid and localized. While I recognize that there’s no silver bullet fix given these complex issues, I’m also keenly aware that there are very real human consequences that spring from poor information handling and governance. My office deals with them daily through our complaints process.

Thank you very much, Mr. Chairman, for your time and consideration. My office staff and I would be happy to answer your questions.

●(0930)

**The Chair:** Thank you very much for your opening statements.

We don't have much time, so we'll move immediately to the Liberal Party.

Mr. Holland, please, for seven minutes.

**Mr. Mark Holland (Ajax—Pickering, Lib.):** Thank you, Mr. Chair.

Thank you very much to the witnesses for taking the time to appear before committee today.

I'm going to start, if I could, with a real concern I have around information sharing. This was really a simple recommendation of Justice O'Connor's report, but what we have heard as we've gone through this process is really no assurance that anything has changed or that Justice O'Connor's recommendations have in fact been implemented.

Mr. O'Brien from CSIS was here and indicated that information was still being shared with countries with poor human rights records. We know that in Justice Iacobucci's report, he indicated that those same practices that were of such concern in the case of Mr. Arar were ongoing and continuing. We had a commitment from the minister stating that he would give a ministerial directive on sharing information with states that use torture, and that it would be forthcoming, and we haven't received it.

This is frustrating, because at the end of the day, the government's chief reason it gives is that we have the Air India inquiry going on, and they don't want to do anything until the Air India inquiry is complete. I'm just wondering if there is anything you feel that inquiry could possibly add to the recommendations already made on the caveats that should be in place with respect to Canadians sharing intelligence with countries that have poor human rights records, particularly countries that are known to torture.

I'll start with Mr. Cavalluzzo.

**Mr. Paul Cavalluzzo:** Just as a private citizen, I read somewhere where a government minister said that all of the recommendations in part one, which would include what you're talking about, have been implemented. I don't know if they have or haven't, but certainly as far as waiting for the Air India inquiry is concerned—and once again I'm speaking as a private citizen—I don't think it would be of assistance, as far as the issue you are talking about are concerned. What we're talking about here is dealing with countries with very poor human rights records, and realistically, as some witnesses have stated before us, in order to get information in respect of particular parts of the world we have to engage with partners that do not have great human rights records. If that's the case, then I think the decision to enter into that kind of a relationship should be a political one. It should not be made by a police agency or a security intelligence agency. I think that's a political question, and all Canadians should participate in that debate.

If we are going to have such a relationship, which realistically I think we have to, unfortunately, then we have to be very careful in terms of the information we send in respect of Canadians. We have to ensure that the information will not in any way be used in respect of human rights abuses. And in respect of information we receive from these agencies, we have to be realistic enough to know the public record, and the public record is that they engage in torture. If we get any information from these foreign agencies, we have to be realistic to understand that it's subject to torture and is likely unreliable, and we had better do a very good reliability assessment on it before we act on that information.

The kinds of issues I've just reviewed really are not part of the Air India inquiry, and there would be no need to wait for the recommendations of Justice Major to deal with those issues, which are very important.

**Mr. Mark Holland:** Before you respond, Ms. Stoddart, maybe I'll just add a couple of comments, to go into the recommendations you made, which I think are very good. Unfortunately a lot of them aren't new. We've seen a lot of them. So in the context of your response, could you address your recommendations and whether or not you feel there's any reason whatsoever that these recommendations should be held off for another inquiry?

I think Mr. Cavalluzzo made an excellent comment with respect to that. If a lot of these are implemented, particularly if the public complaints commissioner has the legislative power to actually be able to investigate, there won't be the need for all of these expensive inquiries that are going to be making the same conclusion.

Again, for the clarity of committee, on the recommendations you made, do you feel in any way that these have to be held back for another inquiry, such as the Air India inquiry?

• (0935)

**Ms. Jennifer Stoddart:** I think, as the honourable member pointed out, these are fundamental principles that are simply being reiterated and positioned for you, ideally, in the network world of modern intelligence sharing. I would think and hope that we could go forward with the necessary review and mechanism agency development without necessarily completely waiting for the results of another inquiry.

However, I would point out, because we appeared and made two submissions to the inquiry on Air India, that what it brings to this discussion is the fact that we have to look at the network world of security intelligence now, and we can't think it's just a matter of maybe the RCMP and the particular cases, and the two previous ones.

What we're also looking at in the Air India Inquiry, I believe, is how national intelligence infects—sorry, it should be “affects”, but perhaps “infects” in some way too—commercial domestic transport: the supervision of our airports, the supervision, for example, of airport personnel. So it brings into the picture the other agencies that are part of the national security world that I think we cannot ignore. And Transport Canada has a role to play. FINTRAC, which does money laundering review, is another part.

So I would say we have to be able to create a model that leaves a place for this kind of development. But I think my colleagues may have—

**Mr. Mark Holland:** Don't misunderstand me—and maybe you can just answer it this way—I think there's an important role for Justice Major to play and important recommendations for him to make. I just don't think the reiteration of the recommendations that you stated here or the reiterations of the recommendations we've heard as a constant refrain over the last four years are something we need to hear again to implement.

Would you agree that the recommendations you're making here and that we heard in Justice O'Connor's report, echoed in Justice Iacobucci's report, echoed in the pension scandal report, are things that we should go ahead and do, and that other things will come out of Justice Major's report that are separate and aside from this that we could act upon once we receive his conclusion?

**Ms. Jennifer Stoddart:** They may be separate and aside, but they're also connected, as I pointed out. Yes, we can go ahead, but we have to leave a place for the important recommendations and what will come out of that report.

**Mr. Mark Holland:** You wouldn't hold back going forward on these recommendations.

**Ms. Jennifer Stoddart:** I think they've been on the table for a long time.

**The Chair:** Thank you.

We'll move to Monsieur Ménard.

[*Translation*]

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

Mr. Cavalluzzo, we were looking forward to meeting with you because we believe that you are familiar with the recommendations from Justice O'Connor and the reasons that led him to make them.

I understand that the part having to do with reparations for Mr. Arar was respected diligently. As far as we are concerned, the most important part of your recommendations deal with the future, recommendations that were made to avoid similar injustices occurring the future.

You have seen what the government has done since the tabling of your report. In this kind of recommendations for the future... We all recognize that not everything was done, but what is the most urgent thing that needs to be done?

[*English*]

**Mr. Paul Cavalluzzo:** I really can't comment whether the recommendations have been implemented. Once again, I'm speaking on my behalf as commission counsel and not on behalf of Mr. Arar. From my perspective, leaving aside part two, the most important recommendations he makes in part one relate to the two things I talked about.

One is information sharing. We see the effects of mislabelling individuals, particularly in foreign countries that are very aggressive as far as terrorist activities are concerned. Inaccurate information, once it's given, is very difficult to take away and remove from the file. Being called a terrorist today is like being called a communist in the 1950s. Once you're labelled a terrorist, it's very difficult to remove that description. On the information sharing, we have to ensure that there are policies in place to ensure the information is reliable and accurate, and that it complies with other laws.

The other important recommendation, which I discussed earlier and I think should be implemented as soon as possible, is the issue of the relationship between Canadian agencies and foreign agencies with poor human rights records. My own view is that any violation of human rights should be dealt with immediately. These are human rights. And if we're aware that foreign countries are abusing the rights of Canadians, we have to ensure and have in place policies that can deal with that situation—and effectively deal with that situation.

Unfortunately, in respect of Mr. Arar's case, there was a great deal of confusion, where different agencies of this country were acting at cross purposes. DFAIT was doing one thing, the RCMP was doing something else, and CSIS was doing something else. We need a coordinated and coherent approach when Canadians are being detained abroad. We have to implement these policies as soon as possible, because this is not a problem that is eliminated at this point in time, as we can see in respect of other situations that are going on today.

• (0940)

[Translation]

**Mr. Serge Ménard:** Concerning the first part, which deals with training for officers so that they use correct, precise and rigorous language, Mr. Zaccardelli assured us that training had been provided very quickly.

In our opinion, one of the major recommendations calls for broadening the authority of the agency that is responsible for oversight of the RCMP. In addition, it was recommended that this authority be exercised by an organization that would integrate more elements, an organization that would oversee the activities of the RCMP, the Canadian Security and Intelligence Service and other organizations.

Should such an organization also oversee the activities of the Department of Transport relating to risk management and the drawing up of a no-fly list? The Canada Border Services Agency needs to have security intelligence to manage both immigration and customs. I think that wasn't mentioned in the O'Connor report. Would you go as far as that?

A recommendation that an integrating organization be in charge of overseeing the activities of the RCMP, CSIS and other entities is certainly very important.

[English]

**Mr. Paul Cavalluzzo:** Yes, unquestionably, that is an important recommendation made by Justice O'Connor. He recommends that the new RCMP body also have jurisdiction over the CBSA, which was involved in the Arar case. SIRC, the Security Intelligence

Review Committee, would have jurisdiction not only over CSIS but also over Transport, CBSA, FINTRAC, and one other agency.

When a problem like Mr. Arar's occurs, Justice O'Connor foresees a complaint being filed with this new committee, and this committee would say, which body or bodies—because we have a number of Canadian entities involved in this—should review this situation? If you don't have review of some of these agencies involved in national security, then you're going to have an accountability gap. As lawyers say, you have to follow the trail, and the trail normally leads from agency to agency to agency.

[Translation]

**Mr. Serge Ménard:** Do you believe that we should wait for the report from the judge who is investigating the Air India attack before we establish these structures?

• (0945)

[English]

**Mr. Paul Cavalluzzo:** As a private citizen and not speaking on behalf Mr. Arar, I would note that Justice O'Connor delivered his last report in December 2006. We are now in 2009, and it seems to me that we have to act effectively. It's up to the government, but I have my own views on that.

**The Chair:** Thank you very much.

Mr. Davies, please.

**Mr. Don Davies (Vancouver Kingsway, NDP):** Thank you, Mr. Chairman, and thank you to all of the witnesses for appearing before us.

I think any right-thinking, rational person would agree that setting up an oversight body is required in this country. I think the efficacy of that depends on a number of factors, including who makes up that committee and how accountable the committee is to oversight, as well, to ensure that it doesn't conduct its own operations so secretly, or with such limitations, that it just becomes another layer of bureaucracy we can't puncture through.

So I want to know if anybody has any thoughts on the makeup of that committee, particularly whether it should be a mix of civilians and those with expertise. I guess what I'm driving at is civilian oversight. I wonder what you feel the civilian presence ought to be on such a committee. And do you have any comment on how we can make sure this oversight committee is responsible to Parliament, and ultimately to the citizens of Canada, to ensure that we ultimately get transparency and accountability through this structure.

**Mr. Paul Cavalluzzo:** Well, I think what is certainly recommended in the Arar report is that the overall coordinating committee in respect of national security be composed of the chair of the new RCMP body, the chair of SIRC, and the CSE commissioner, as well as an independent person who would chair the committee. That independent person, hopefully, would be someone who has a great deal of respect within the community, because as you say, transparency and accountability are important to these review mechanisms, particularly in the national security area. Those are the two important values.



As far as the individual bodies are concerned, I think SIRC is a good model for the new RCMP body. As we know, SIRC is composed of independent people who are normally former politicians or cabinet ministers with a great deal of public policy experience, who have the respect of the public; and as a result of that, what they do gains public confidence. The CSE commissioner is normally a former judge of the Supreme Court of Canada, who obviously has the respect of the community. So I think we need people like that who would gain public respect.

As far as legislative oversight is concerned, I think these bodies should be responsible to this committee, as well as to the Senate committee, on an annual basis, or on call by this committee when you feel something has to be reviewed, so that we have an independent arm of the executive responsible to a legislative committee and ultimately to Parliament, which is, of course, the parliamentary system in which we exist.

Thank you.

**Ms. Jennifer Stoddart:** Could I add to that, honourable member, that it's not just who's on the committee, who the committee reports to, but what the committee can do. What are its powers?

I think one of the reasons we have diagnosed that the public complaints committee against the RCMP has not been effective historically is that it depends on public complaints. I can echo that, because I also have complaint investigation powers, but if I only had that in terms of what I could do with my mandate, I would be a lot less effective.

So it is extremely important that this committee can take on initiatives, have audit power, compel production, and define the issues that are going to be reviewed by the committee.

I'll give an example of some of our recent work. In the federal government we have audit power. Following the beginning of the O'Connor inquiry, at about the time we appeared, we began a review of the RCMP exempt banks. Exempt banks are banks where people ask, am I in the bank? Is there a government file on me? And the RCMP don't have to answer. It is secret.

What we did find out in a special report we laid before Parliament was that the RCMP, in spite of what was going on in the Arar inquiry, had neglected to clean out these banks to see whether all these citizens.... There were I think thousands of innocent citizens who found themselves in these exempt banks and therefore possibly could show up on police files as people of interest, but they weren't allowed to know why they were in there.

My whole report was laid before Parliament, and I am sure the members are familiar with it.

But without that kind of power, you cannot go and look in the dark corners to see what might be hidden under the dust.

• (0950)

**Mr. Don Davies:** Thank you.

I'll probably direct this question to Mr. Cavalluzzo.

I worked with privacy legislation in my previous life. In my view, the main goal of privacy legislation is to ensure that our private information does not get disseminated improperly to people who

ought not to have it. But several times in the testimony I heard a reference to inaccurate, misleading information being disseminated and shared with other countries. What is particularly disturbing to me is that it is not normal, accurate information for which I have a privacy interest that was shared; it was inaccurate information. This was information given by our national police force. They are supposed to be professional investigators.

Can you comment on how that happened?

**Mr. Paul Cavalluzzo:** With the new anti-terrorism legislation the RCMP was given new national security responsibilities. You may recall that in 1981 the McDonald commission said the RCMP should get out of the national security game, and that is why we created CSIS. In any event, we brought them back into the national security game in 2001, and there was very little training for these front-line officers in national security issues.

As a result, these were good police officers, but they had no idea of the impact of the exchange of this kind of information, particularly with the Americans, and they had no idea that just because a piece of intelligence says this guy's neighbour says he's a member of al-Qaeda, you can't rely on that, that this is just information or intelligence. You have to analyze it, you have to corroborate it, and so on. Before you send any information like that, you'd better be sure it's accurate.

So for the most part it was really, unfortunately, a lack of training. I don't think there was any malfeasance, but certainly these people were not competent to be sharing that kind of information.

**The Chair:** We'll have to move to the government side now.

Mr. Rathgeber, please.

**Mr. Brent Rathgeber (Edmonton—St. Albert, CPC):** Thank you, Mr. Chair, and thank you to all the witnesses for your attendance today and for your expertise.

I find this topic quite fascinating and also very troubling, and I certainly share some of the concerns of my friend Mr. Davies. I too have some background with respect to freedom of information and protection of privacy. I chaired the review of the Alberta statute in the Alberta legislature.

Picking up on his question about inaccurate information, maybe this is just purely semantic or definitional, Ms. Stoddart, but I agree with his concern. Does personal information apply to information that is inaccurate? For example, I do not have a criminal record. If somebody were to disclose that I did, is that considered to be my personal information? Because it is not my personal information. It is wrong.

**Ms. Jennifer Stoddart:** You hit on a very important point there, honourable member. One of the bases of not only the Privacy Act but generally fair information principles is that the information about an individual has to be accurate. That individual, in democratic societies, has to have the right to have that information corrected. That's in fact a large part of what our office does.

What we see here are very particular cases of inaccurate personal information, unverified—and this is from the Iacobucci report and I believe the Arar report—being shared in a rather informal fashion. Again, it's not consistent with fair information principles about a very strict definition of the use to which you put personal information and accountability for the use of that personal information subsequently put.

This is one of the reasons that I think Privacy Act reform—Privacy Act applies to all the government agencies—is so important to give citizens a broader right to complain about inaccuracy of their personal information and, if the information is not corrected, to take it on to Federal Court. Right now, they don't have that right. It's a very truncated right. If they had had this kind of right, some of these cases may in fact have taken another turn of events.

• (0955)

**Mr. Brent Rathgeber:** Thank you.

In your opening comments, you quoted from Ms. Bloodworth, talking about privacy rights of citizens and ensuring physical security. You went on to make an interesting statement, that not only is this the greatest single issue that our Parliament must confront, but that security and privacy are not mutually exclusive.

I'm troubled by that concept. I certainly agree that both privacy and national security are invaluable goals that we must promote. But how can they not be mutually exclusive? I would suggest that in the unfortunate circumstance of Mr. Arar, an overzealous attempt to promote national security severely jeopardized and compromised his privacy rights and ultimately his human rights. In other situations, we could quote anecdotally that protection of privacy rights might have compromised national security.

I'm curious as to how they cannot be mutually exclusive, although I agree with you that they're both goals that ought to be zealously promoted.

**Ms. Jennifer Stoddart:** What I'm saying is that we don't have to continue to think about them as always being mutually exclusive. That's the challenge of the society that we live in. We have to protect our citizens. That's probably the number one role of government right now—physical security, integrity, safety. Those are basic human rights. Also, a basic human right is privacy, which means autonomy, which means freedom, which means our sense of liberty.

We have to organize, in our society, our processes and our laws in new ways to preserve them both so that one intrudes the least possible on the other. This is the challenge, because in the late 20th century Canada was fortunate in having a minimum of national security threats. Our privacy just came naturally because we were not a society under any kind of threat, compared to other societies where there were long histories of wars, invasion, persecutions, and so on. As we go forward, I am saying they are not in themselves, by nature, always mutually exclusive. That's what we have to aim to do.

**Mr. Brent Rathgeber:** I'm going to have to think about that a little bit more, but thank you.

Mr. Cavalluzzo, I read Justice O'Connor's report, or at least most of it, with great interest. I have a couple of questions on the creation of the independent complaint review committee.

First, why not just expand the role of the existing RCMP complaints committee, Mr. Kennedy's committee?

Secondly, I'm asking about your opinion or maybe his opinion vicariously through you. With all of these different committees—SIRC and the independent complaints review committee that Justice O'Connor recommends the creation of—how does that promote the coordinated and consistent approach you talked about? It appears to me that it's still a hodgepodge of different jurisdictions and different agencies.

**Mr. Paul Cavalluzzo:** Okay, in respect of Mr. Kennedy's committee, what Justice O'Connor talked about was a restructured CPC, so that the new independent review committee would have much broader powers than the CPC, including national security, as well as just general law enforcement powers, and that would be the new RCMP committee. So it's a restructured Kennedy committee, with much broader powers.

On the second point, in terms of coordination, the point once again of this new committee.... This isn't the RCMP committee, but there would be a broad coordinating committee, which would be composed of the chairs of the new RCMP body, SIRC, and the CSE commissioner, and national security complaints would be filed with this new coordinating committee. And the new coordinating committee would look at the complaint and say, "I think SIRC would be the body to deal with this", or he or she might say, "This involves the RCMP as well as CSIS, so I think both CSIS and the RCMP new committee should conduct a joint investigation." And certainly there would be new legislative gateways so that these bodies could act together, exchange information, and conduct joint investigations.

Where Justice O'Connor went to school, so to speak, on this is that there are foreign committees that conduct these kinds of joint investigations, and that way you have total control of the integrated investigation that has gone on, because there will be one committee acting—or could be acting— together that would cover all of the Canadians that are engaged in national security.

• (1000)

**Mr. Brent Rathgeber:** Thank you.

I suspect my time is done.

**The Chair:** Yes.

We'll move over to Mr. Oliphant now, please.

Five minutes.

**Mr. Robert Oliphant (Don Valley West, Lib.):** Thank you.

And thank you, again, for being with us today.

With all due respect to my colleagues across the way, without wanting to get into a sermon, I wanted to quickly raise three points.

Despite having read the report...this report is simply not about sharing of information in general that may be government information; this is about sharing wrong information, misleading information, inaccurate information, and damaging information that has hurt people's lives. Recommendation after recommendation in Justice O'Connor's report is about people who are Canadians.

That falls into my second point, which is that not only are privacy and security not mutually exclusive, they're intimately bound together and cannot be released from each other. We are not safe if we do not have the ability to have our privacy protected. We have a false sense of security. It's not that they're possibly not mutually exclusive; they are absolutely entwined with each other or our Canadians are not safe.

That's the end of my sermon. Excuse me. Amen. I want to preach.

I'll get to my question. The bulk of this report is about privacy and information. The bulk of the recommendations have to do with information and inaccurate sharing of information. That puts us into the concept of labelling and what happens when people are labelled, which is bad enough, but when we share the labelling with either agencies within this country or, worse, outside this country with partners who are not dependable, we have a huge problem. And the report is very clear, in recommendation 5 I think it is, that the minister should be issuing ministerial directives to ensure that labelling does not take place by the RCMP or any of the other agencies that are involved in this.

Are you aware of any ministerial directives that have been released since 2006—we're now in 2009—since this report was issued?

**Mr. Paul Cavalluzzo:** I am not, but that doesn't mean it hasn't happened. I'm in private practice now, doing other things, and so I'm not aware of whether such a directive has been issued. Certainly there was a recommendation that it be issued, but I'm not aware of it.

**Ms. Jennifer Stoddart:** Yes, I'm aware, and I'd ask maybe Mr. Baggaley if he could talk to this.

I believe Treasury Board is working on a directive of this kind, because members of my staff have been consulted.

**Mr. Carman Baggaley (Strategic Policy Advisor, Office of the Privacy Commissioner of Canada):** What I wanted to comment on was that Justice Iacobucci specifically raises the issue that you referred to. In fact, one of his findings is to suggest that in fact it's a practice to send information to another country labelling someone as an Islamic terrorist, or something else, as a kind of fishing expedition to determine whether or not the receiving country can either confirm or deny that allegation. Although Commissioner Iacobucci doesn't make any recommendations in his report, as you may know, he comes very close to suggesting a recommendation, and he strongly disapproves of that type of practice where it's done deliberately. It's not being done because they're not quite sure, but according to the justice, it's being done as a kind of fishing expedition.

**Mr. Robert Oliphant:** My concern is that the labelling practices that we became aware of as a result of O'Connor and Iacobucci continue to this day, and this is affecting my constituents. They and their families are labelled when they try to cross the border and when they're met by CSIS agents, who want to interrogate them about

issues constantly. It's a practice that I think is extremely dangerous for our security. I think it's intimately related to our security, because if one Canadian is not safe, we're not safe as a society.

It seems to me that the Office of the Privacy Commissioner has to constantly be vigilant on this issue, as you are, but what else can we as a committee do to help you do this work that we value so greatly? You're suggesting we have more resources to do our work; what else can we do to be supportive of you and to protect Canadians?

• (1005)

**Ms. Jennifer Stoddart:** By raising the issues and by raising interest in the various aspects of privacy—and there are many—parliamentary committees in the last few years have helped to make Canadians much more aware of their privacy rights and how they can be improved, so we certainly appreciate your attention to the issues and the recommendations that come out of the various committees. For example, our own ethics committee on Privacy Act reform would have an impact on the issues we're discussing here, because one of the things I hope they recommend is to put in a necessity test for collecting information. This is a basic principle of fair information—principles around the world. If there had been a necessity test applied to the use of the collection of information by national security agencies, we might have another story today.

**The Chair:** Thank you.

Mr. McColeman, please go ahead.

**Mr. Phil McColeman (Brant, CPC):** I want to thank all of you for coming and sharing your expertise. Certainly the depth of knowledge is extensive here, and we're learning a lot in trying to move towards doing the right thing by protecting public safety while balancing the rights of individuals.

Although it really wasn't the direction I was going to go in, I'm interested in following up on the commissioner's comment on the necessity test.

You said earlier that the first violation was the violation to their privacy, if I might paraphrase what you were saying. What is the test of crossing the line on privacy? Is this the necessity test that you just referred to?

**Ms. Jennifer Stoddart:** There are many components of fair information, which is part of our privacy. Our privacy can have many dimensions, but in terms of information about us, you go through the sequence of how the information circulates about us. One of the fundamental principles is that an organization collects only the information it needs, not just any information it can Hoover up, any information it might find about you that it would keep just in case it could be useful some day. The principle is to collect only the information that is actually needed, because it is actually your private information.

Then we go on to other principles, such as the requirement for the information to be accurate and up to date. You only share it for purposes that are, as our own Privacy Act says, consistent; that is, they're roughly equivalent, or they're compatible with, the reason for which it was initially collected.

All this is to prevent government agencies or the government itself from turning us into a surveillance state that has all kinds of information on individual Canadians that it can't justify.

**Mr. Phil McColeman:** I appreciate where you're going on this continuum of a police state in which we collect too much information on individuals, but let me suggest something to you and get your reaction.

Part of my experience was on an oversight body for police services in my community. The reality in a lot of situations is that because we are human, there's going to be human error, and this human error is going to mean that sometimes bad things happen that shouldn't happen to people. That's unfortunate. I'm not diminishing any of the reports that have come out, but I'd like you to address that and assist this committee in terms of your thinking on this continuum, because the collection of information, the determinations, and the judgments made as to whether we should go down this road or another road are all subject to errors by individuals and to human error along the way.

I don't think we can have a playbook saying that if this happens you do this, and if this happens you do that. What are your thoughts as to where you strike this balance or determination on where you head with information?

• (1010)

**Ms. Jennifer Stoddart:** Could I ask Assistant Commissioner Bernier, who is a specialist on the Privacy Act, to answer?

**Ms. Chantal Bernier (Assistant Privacy Commissioner, Office of the Privacy Commissioner of Canada):** I would say that it is precisely the reality of human error that begs for oversight, review, remedies for correction. As the commissioner said before, privacy rights include the right to accurate information as well as the right to have inaccurate information corrected, so your own statement is precisely the basis for the necessity of proper oversight mechanisms, which is what we are putting forward.

**Mr. Phil McColeman:** I'll probably have time for one last question here.

We had representation from the British Parliament on their oversight mechanism for national security. Are you familiar with that model? This is one whereby the Prime Minister appoints senior parliamentarians, people who really have no agenda to move through the political process, because as you can see from our interaction here, things become politicized very easily at this level. In a serious matter such as national security, I wish it weren't that way, frankly. I speak for myself here.

Having said that, the British model is one in which these parliamentarians operate in a fairly secretive environment. They get the very details of what has happened and have to be sworn to secrecy on a lot of these matters. They're hand-picked by the Prime Minister and report to the Prime Minister of Britain.

What do you think of that model?

**Ms. Chantal Bernier:** I am familiar with it and in fact have had the privilege of meeting them as well.

We have discussed it at the OPC. We feel that its transferability to Canada must be assessed by the competent authorities. If such a proposal were to be put forward, we would obviously look at it through the lens of the Privacy Act. We do not have a position at this stage.

**Mr. Phil McColeman:** That's interesting. Thank you.

**The Chair:** We'll have to wrap it up there.

Monsieur Ménard.

[*Translation*]

**Mr. Serge Ménard:** Thank you.

It's funny, but at the very end, if I had had the time, I would have asked the question that my colleague just asked. Perhaps I could talk to you about this right now.

The O'Connor report does not contain any suggestions in this regard. Even so, there was a bill tabled by Ms. McLellan of the previous government, which was intended to set up this kind of committee. Since then, nothing has happened.

Concerning the questions from Mr. Oliphant, I think it is essential for us to categorize people that police officers are investigating. Be it investigations into organized crime or more of an investigation relating to national security, when the police suspect people, it is important for the other police forces to know that these people are under suspicion. Even if the police officers do not yet know whether the suspicions are justified or not, suspects must be categorized when criminal intelligence is being analyzed.

For example, we talked about persons of interest. In my opinion, Mr. Arar was one. However, there are thousands of people of interest who are not terrorists. If we met them under other circumstances, or if we observed them, we could verify if there was something else that could justify taking them from the "person of interest" category and placing them in the "suspect" category, or moving them from the "suspect" category to the "confirmed person" category or the "people we are sure of" category.

I would like to hear Ms. Stoddart's opinion on this. In my opinion, such categories should remain secret, because if the person has been put in the wrong category, and if we want investigations to go somewhere, we must not let people know that they have been slotted into a particular category and are under investigation. Such suspicions can be passed on to other countries or to agencies of other countries.

**Ms. Jennifer Stoddart:** In my opinion, you have raised an important issue, namely, the type of categorization that both the police and people working in national security need to do. The message that I would like to give you today is not that any type of categorization is prohibited under the Privacy Act, far from it. It is absolutely essential that our security forces do this type of classification. The problem that we have raised and which results in a contravention of the Privacy Act and in a breach of citizens' rights occurs when categorization is inaccurate and false.

I will go back to my example of the review we did pertaining to the RCMP's exempt data bank, which existed at the same time that the Arar Commission was doing its work. If we had not had the authority to audit that exempt bank, there would have been all kinds of inaccurate audits, and the name and identity of several thousand Canadians would have ended up in an exempt data bank, because these individuals would have been persons of interest to the RCMP. When we began our audit, the RCMP was the first to admit that this data bank had not been cleaned up. It's possible—and we were not able to ascertain whether or not this was the case—that there were repercussions for individuals whose name had been in this bank for five or six years at the time of the audit.

I completely agree with you that we need to move persons from one category to another, but this has to all be based on facts.

● (1015)

**Mr. Serge Ménard:** One thing we can certainly agree on is that it's also important that rigorous practices be adopted, not only to ensure people's safety but also to protect them from unfair suspicions. That's what was missing in the Arar case, which, as we well know, had a disastrous outcome. I believe that in the other three cases as well, the process lacked rigour from the outset.

Ms. Stoddart, I would like to know your opinion of the practice of disclosing the legal files of Canadian citizens to other countries. In your opinion, should we be readily sharing citizens' legal files, using the quickest methods available, like the computer? If not, what precautions should be taken before such disclosures are made?

[English]

**The Chair:** Please be very brief.

[Translation]

**Ms. Jennifer Stoddart:** Under the terms of the Privacy Act, there has to be an agreement or an arrangement. In the work that my office has been doing in the area of national security, we have noted that, over the past five years, there often has not been clearly defined parameters. Rather, we have seen informal exchanges whereas the legislation more or less says that the agreement needs to clearly define what can be exchanged and why. Informal exchanges that happen on the spur of the moment, without any forethought, can pose serious privacy risks.

[English]

**The Chair:** Thank you.

We'll go to Mr. Richards now, please, for five minutes.

**Mr. Blake Richards (Wild Rose, CPC):** Thank you. I appreciate your being here today.

Obviously privacy issues are very important; privacy is one of the important rights that we as Canadians enjoy. Of course, we have to balance this right with others, such as the right to safety and security. I'm sure you're well aware of that. I appreciate the detail and the thought you've put into some of the recommendations you've brought forward to us today.

Of course, when we look at recommendations such as these, we always have to be mindful of the costs involved. When I say that, I talk about not only financial and logistical costs, but also the opportunity cost. As an example, for every minute that the RCMP

spends on paperwork or ensuring that we're not unduly invading anyone's privacy, there is an opportunity cost to it; it gives away some of their time that could be spent investigating. We always have to be mindful to make sure we find the right balance.

That's where I want to go with my questions to you. I'm sure someone who has put as much thought and detail into recommendations as you has certainly thought about those logistics and the costs, including opportunity costs, involved.

I will point to just a few of the recommendations in your report: talking about requiring within security agencies enhanced training around the theory and practice of privacy; appointing chief privacy officers across government; providing the Commission for Public Complaints Against the RCMP with the resources required to deal with privacy issues; talking about the Treasury Board and ministers issuing new policy requirements for their departments, especially around thorough privacy impact assessments; talking about increasing the resources of committees such as this one and the Senate committee. These things all have costs, be they financial costs or opportunity costs.

I'm wondering how much thought you have put into what kind of new resources would be required to implement these recommendations and how much these recommendations would cost, and whether you have thought about their implications in terms of balancing privacy with other activities that these bodies and agencies can and should be doing as well. Give me a bit of a sense as to what you see the cost here being, in terms of resources, finances, and also opportunity costs.

● (1020)

**Ms. Jennifer Stoddart:** Okay.

**Mr. Blake Richards:** I know that's a broad question to ask. Maybe you want to focus on one or two of the recommendations I've indicated.

**Ms. Jennifer Stoddart:** Yes, thank you.

Mr. Chairman, my office isn't really equipped to evaluate the cost of these various recommendations. I believe the Treasury Board is.

Perhaps the point I could make to this committee is that the opportunity costs are the important factor to look at. If we had invested in, for example.... Mr. Cavalluzzo mentioned that in 2001 the RCMP, having been out of national security, all of a sudden—whoops!—came into the field, and the people were not trained. If they had been trained in information management practices and if there had been a chief privacy officer, perhaps much of the saga that in the end was very costly to the Canadian public might have been avoided.

I think my colleague wants to briefly add something.

**Ms. Chantal Bernier:** I would submit to you, first of all, that we need to talk about or at least consider the cost of not doing it.

Secondly, we know, for example, that since the advent of the Charter of Rights and Freedoms, we have seen that the added rigour that consideration for human rights brings to police investigations has, indeed, added a gain in efficiency both in terms of cost and opportunity, as you suggest.

**Mr. Blake Richards:** Could you give me some examples of how that is in fact the case? I'm not disputing that it is, but—

**Ms. Chantal Bernier:** For example, a police officer will not inundate himself or herself or a file with unnecessary information, but will be much more focused, that focus perhaps being initially brought on by considerations for privacy, but leading to a much more efficient investigation process.

**Mr. Blake Richards:** I'm not disputing what you're saying at all, but there are always two sides to the story. That could be true, and I think it may very well be, but there also could be the other side of it: that sometimes it may be they're spending time being concerned about ensuring privacy, and this takes away some of the information they could have used in an investigation.

**The Chair:** We'll have to wrap it up there. I'm sorry. We have eight minutes left. Can we split it—four minutes and four minutes?

Mr. Kania, go ahead.

**Mr. Andrew Kania (Brampton West, Lib.):** Madam Stoddart, in your May 7, 2009, submission, "Rights and reality: enhancing oversight for national security programs in Canada", you indicated that "The recommendations from the O'Connor Policy Review have yet to be implemented". Are you aware of the fact that the government takes the position that they have all been implemented except for the overall supervisory organization?

I have a quote here. As far back as when Stockwell Day was the public safety minister, he indicated, in responding to Commissioner Iacobucci's report, that O'Connor's recommendations have, in fact, all been implemented. He also stated that there had been considerable progress towards designing a new model for review, on which there would apparently be a public announcement in the near future. That was when Stockwell Day was public safety minister.

I'm wondering if you have seen any evidence of any implementation of any of the three recommendations.

**Ms. Jennifer Stoddart:** I am aware of the differences of opinion between my statement and the government statements. That's from our various perspectives, I being a parliamentary watchdog agency.

What I mean is that the recommendations have not been fully implemented, and we do not see them being operational. We do not see any kind of oversight and review committee, which is the main focus of my message to you today.

I am aware, however—and I think in that sense it explains the government's position on this—that work is being done on this. Work is being done within the government. I mentioned that we had been consulted on draft directives for more appropriate information sharing within the government. We also have been told that work is being done within Public Safety Canada on an oversight committee.

Indeed, my colleague, who was there until six months ago, can speak to that.

•(1025)

**Mr. Andrew Kania:** You would all presumably agree with me that when former Minister of Public Safety Stockwell Day indicated, quite some time ago, that all the recommendations were implemen-

ted, that would not have been accurate. Would you all agree with that comment?

**Ms. Jennifer Stoddart:** I have not seen all the recommendations from the O'Connor inquiry implemented, some of which had to do with a committee that I don't believe is in existence.

**Mr. Paul Cavalluzzo:** I think we have to be cautious here. I don't know if Minister Day was talking about part one. If he was talking about part one, then perhaps all those recommendations have been carried out. As far as part two is concerned, clearly that hasn't happened.

We have to look at the context of his statement as to what he was talking about.

**Mr. Andrew Kania:** Let's discuss that. Obviously part two has not been implemented. We all know that.

**Mr. Paul Cavalluzzo:** That's correct.

**Mr. Andrew Kania:** In terms of part one, do you have any proof or evidence that they have been implemented?

**Mr. Paul Cavalluzzo:** No, other than the statement of a cabinet minister, and I would rely on that statement.

**Mr. Andrew Kania:** Other than that individual's statement, there's nothing else you have.

**Mr. Paul Cavalluzzo:** That's correct.

**Mr. Andrew Kania:** Let's assume, because we see no evidence that they've been implemented, that they've not been. Are you aware of any new cases or rights abuses that have taken place since these reports?

What I'm trying to get at is that these recommendations have not been implemented. Obviously they were made to prevent further abuses. As a result of the failure to implement, are you aware of any other cases that have arisen?

**Ms. Jennifer Stoddart:** I would simply say that we do have ongoing complaints against many organizations with national security mandates, but I do not know...and the nature of our regime is that I can't speak of the contents publicly. Certainly we have complaints on an ongoing basis against many of the organizations we've discussed today.

**The Chair:** Thank you very much.

We'll go to Mr. MacKenzie, please.

**Mr. Dave MacKenzie (Oxford, CPC):** Perhaps you can see why the British system might not work as well here as it does in Britain.

Is that not the nature of your work, to investigate ongoing complaints?

**Ms. Jennifer Stoddart:** Yes, absolutely.

**Mr. Dave MacKenzie:** If we go back to the Air India inquiry that's ongoing, one of the issues raised in that was the lack of information sharing between the federal agencies, and so on. Are there things we can learn and should learn and perhaps have learned from that particular inquiry in a public sense of why we need to improve information sharing among our agencies as opposed to limiting it?

I understand the need for privacy, but I think there is a need for sharing.

**Ms. Jennifer Stoddart:** Yes. I don't disagree with that.

I can't prejudge what Mr. Justice Major may be saying in his report; however, I did find very instructive the recent report of the Auditor General, which I think is very illuminating on this question and which highlighted the need for intelligence sharing. Highlighted also was the fact that some recommendations she made in an audit in 2003, I believe, had not been followed up on.

Highlighted also was the misuse of the Privacy Act, which is a great concern of mine, in that the Privacy Act is quoted as a reason for not sharing intelligence among national security agencies. When the Auditor General asked where the legal opinion was or where the memorandum was and how they analyzed the Privacy Act such that they thought it prevented them from sharing information, there were none of these documents.

I think that's an important part of the puzzle that we have to look at. It's not only that the Privacy Act be respected, but possibly that the Privacy Act be refocused to be more contemporary, and also that it not be used wrongly as a shield against necessary information sharing.

• (1030)

**Mr. Dave MacKenzie:** One of the witnesses before the Major inquiry who was from the Canadian banks, which are mandated to provide information through FINTRAC, indicated, I think, that there was an issue about their feeling that they were in the dark. They must provide the information, but there's no sort of feedback, if you will, or whatever.

There's a sense that there's a big package there that is worthwhile, and that it is worth their time and effort to do it, but that sometimes we get caught up—and rightly so—in being concerned about privacy. Sometimes we make it so secret that the folks whose cooperation we need in a general sense feel that perhaps we've gone too far one way.

I don't know whether you have any comments.

**Ms. Jennifer Stoddart:** I think my colleague has some thoughts on that.

**Ms. Chantal Bernier:** Indeed, as the commissioner has said, we would refer you to the March 2009 Report of the Auditor General, wherein she specifically raises that issue and says that the Canadian population will trust the national security and intelligence organizations only if it knows that they have maintained the proper balance between privacy and national security. She goes on to say that this proper balance has not been struck due to a lack of guidance to the departments and agencies concerned.

I can tell you what we are doing at the moment in this regard. You've mentioned FINTRAC. We are about to complete an audit of FINTRAC. We are mandated by law to do so, and it is about to come out, so you will certainly want to turn your attention to that.

In 2006, we did an audit of CBSA. We are following up on it now and we are addressing, in that context, information sharing agreements. We are also working with Treasury Board, as my colleague Carman Baggaley and the commissioner have said, on developing guidance on information sharing. This guidance will contain provisions on transborder sharing of information.

Finally, we are also reviewing the very recent Transport Canada-RCMP agreement on information sharing from the point of view of privacy.

**Mr. Dave MacKenzie:** I think that at one point you were perhaps going to answer my colleague across the aisle when there was an issue about whether anything had been done, and I think Ms. Stoddart indicated that in your previous home you perhaps had more knowledge about how some of those things may have been done.

I know that we simply don't have the time, but I'm quite satisfied that it isn't the case that nothing's been done; there has been a great deal done. Maybe it's not complete, but there has been a great deal done, and I know it's through the work of people like you, so thank you.

**Ms. Chantal Bernier:** Thank you.

**The Chair:** I'd like to thank the witnesses. We'll end this portion of our meeting. We're going to suspend for a minute or two.

Again, thank you very much. We're going to have to clear the room because we're going in camera.

*[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.**