HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 040 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, December 8, 2016

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Thursday, December 8, 2016

● (1100)

[*English*]

The Chair (Mr. Blaine Calkins (Red Deer—Lacombe, CPC)): I call the meeting to order.

Good morning, colleagues.

We are at our 40th meeting of the Standing Committee on Access to Information, Privacy and Ethics. We are resuming our study of the Security of Canada Information Sharing Act, otherwise known as SCISA.

We are delighted to have witnesses with us today, from the Office of the Communications Security Establishment Commissioner, Mr. Jean-Pierre Plouffe, who is commissioner. With him is Mr. J. William Galbraith, the executive director. From the Security Intelligence Review Committee, we have Pierre Blais, who is the chair, and Ms. Chantelle Bowers, who is the deputy executive director. From the Civilian Review and Complaints Commission for the Royal Canadian Mounted Police, we have Mr. Richard Evans, who is the senior director of operations, and Ms. Joanne Gibb, acting director, research, policy and strategic investigations unit.

Welcome, all, and thank you very much for being here today.

I'm sure none of you are rookies at appearing before a committee, so you know exactly what's going to happen. The translation devices are there. The committee's routine proceedings and standing orders allow for 10-minute presentations from each group. How you want to use that time is up to you. If only one person wants to do all of the talking, that's fine. Then we'll proceed to several rounds of questions and answers. We'll encourage you to be as insightful as possible, but as succinct as possible at the same time. I appreciate you all being here this morning.

We will start with the Office of the Communications Security Establishment Commissioner.

The floor is yours, Mr. Plouffe.

[*Translation*]

Mr. Jean-Pierre Plouffe (Commissioner, Office of the Communications Security Establishment Commissioner): Thank you, Mr. Chair and honourable members.

[*English*]

I am pleased to appear before this committee on the subject of the Security of Canada Information Sharing Act. As the chair has mentioned, I am accompanied by Mr. Bill Galbraith, the executive director of my office.

Before I make a few remarks about activities under this act, and since this is my first appearance before this committee, I will very briefly describe my mandate and the role of my office.

[*Translation*]

You have my biographical note, so I won't go over that, but I would like to say that I have found that my decades-long experience as a judge has stood me in very good stead in my three years as CSE Commissioner.

Being a retired or supernumerary judge of a superior court is a requirement set out in the National Defence Act, the legislation that mandates both my office and the Communications Security Establishment.

The CSE Commissioner is independent and arm's length from government. My office has its own budget granted by Parliament. I have all the powers under Part II of the Inquiries Act, which gives me full access to all CSE facilities, files, systems and personnel, including the power of subpoena, should that be necessary.

[*English*]

My mandate is threefold. First, I review the activities of CSE to determine whether they are in compliance with the law, including protecting the privacy of Canadian citizens. This is the major portion of my work. Second, I may receive and investigate any complaints I consider necessary. Complaints are rare, reflecting the foreign focus of CSE activities. Third, I have a duty to inform the Minister of National Defence and the Attorney General of Canada of any activity of CSE that I believe may not be in compliance with the law.

The commissioner's external, independent role, focused on CSE, assists the minister responsible for CSE—that is, the Minister of National Defence—in his accountability to Parliament, and subsequently to Canadian citizens, for that agency. My annual report tabled in Parliament describes the results of my reviews.

Let me turn now to the Security of Canada Information Sharing Act, or SCISA. What I have to say will be relatively brief. I will describe to you the experience of my office with respect to SCISA and then make a number of brief points regarding the act.

First, my office, as a government institution, has not shared information under SCISA, and in all probability is unlikely ever to do so. During the first year that SCISA was in effect, the agency I that review—namely, the Communications Security Establishment, or CSE—has neither received nor shared information under that law.

My reviews of CSE include CSE information sharing with domestic and international partners. I review CSE activities to ensure that the information it collects and discloses complies with the law, ministerial direction, and internal CSE policies. This includes ensuring that satisfactory measures are in place to protect privacy and that these measures are effectively applied. I will continue to monitor whether CSE receives or shares any information pursuant to SCISA.

That CSE has neither received nor shared information under SCISA demonstrates that currently existing authorities are sufficient for it to share or disclose information with other government institutions.

● (1105)

[*Translation*]

The point was made more broadly in the annual report of the Privacy Commissioner, Mr. Therrien, noting from a survey of government institutions his office conducted of the first six months SCISA was in effect, that only five institutions either received or shared information pursuant to the act. Most institutions, a little like CSE, have been using pre-existing authorities.

[*English*]

I cannot answer if in the future CSE would receive or share information under SCISA, but the track record to date suggests little, if any. As I said, I will monitor this.

As to the act itself, there are three points I would comment on. These points were also raised by the Privacy Commissioner in his testimony before this committee, and I must say that I am in general agreement.

First is the question of threshold in order for information to be shared. In SCISA the threshold is relevance, and I quote from subsection 5(1) of the act:

> if the information is relevant to the recipient institution's jurisdiction or responsibilities

Where personal information is concerned, in my view the threshold should be higher. The Privacy Commissioner suggests necessity as a threshold. He states that this an international privacy standard, noting that the CSIS Act uses the threshold "strictly necessary" for CSIS to collect, analyze, and retain information.

[*Translation*]

Another example can be taken from the National Defence Act, where the established threshold is essentiality. In essence, in order for CSE to use and retain a private communication—where one end is in Canada—collected under ministerial authorization, CSE must determine whether the private communication is "essential". I review these communications to ensure that is the case, and that information that is not "essential" has been destroyed.

● (1110)

[*English*]

The next point with regard to SCISA relates to safeguards to protect privacy. Given that CSE has not received or shared information under SCISA, I have no direct experience with this act in this regard. However, I can comment that the legislation mandating CSE has built-in privacy safeguards. These safeguards require CSE to have satisfactory measures in place to protect any information with a privacy interest that it can legally collect, retain, and use. I would agree with the Privacy Commissioner that there should be safeguards in SCISA to ensure protection of personal information.

[*Translation*]

A third point relates to the government institutions listed in Schedule 3 of SCISA. Only three of the 17 institutions listed in Schedule 3 are subject to expert review: CSE, which I review; CSIS, which is reviewed by my colleagues from SIRC; and the RCMP, reviewed by my colleagues from the Civilian Review and Complaints Commission, where Mr. Evans works.

[*English*]

The Privacy Commissioner has a mandate to review personal information policies and practices of all federal government institutions. In this context, Mr. Therrien is examining the schedule 3 institutions' use of SCISA and privacy protections. However, this is not enough. I suggest that there is a need for expert review for the 14 institutions not currently subject to review. This could be done either by a new review body, or bodies, or divided among the existing expert review bodies, much as recommended by Justice O'Connor in his commission of inquiry report 10 years ago in the Arar affair.

Perhaps there is a role here for the national security and intelligence committee of parliamentarians. The committee will have to establish its priorities, and this may be one area to examine. I look forward to working closely with the committee of parliamentarians and its secretariat.

Thank you for this opportunity to appear before you today. My executive director and I would be pleased to answer your questions.

[*Translation*]

We will be pleased to answer your questions to the best of our knowledge.

Thank you.

[*English*]

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

We now move to Mr. Blais, for up to 10 minutes.

Hon. Pierre Blais (Chair, Security Intelligence Review Committee): Good morning, Mr. Chair and members.

Thank you for providing this opportunity to appear before you today in the context of your study of SCISA—I will not repeat the long name, either in French or in English—and specifically its impact on privacy and any desired changes in light of the national security consultation and review process that is currently under way.

[*Translation*]

Today, I hope to enrich your study by focusing on three key points.

First, I will briefly outline SIRC's work in reviewing CSIS's information sharing practices with domestic partners. Second, I will provide insight into SIRC's current review examining the impact of the Security of Canada Information Sharing Act, or SCISA, on CSIS's information sharing with domestic partners.

Third, I will explain SIRC's limitations when examining these exchanges, including those made under SCISA.

[*English*]

I will not take much time now to describe SIRC's mandate and responsibilities. I will be pleased to answer any questions about our work following my remarks.

I will simply state that SIRC is an independent external review body that reports directly to Parliament, as you know, on CSIS activities through an annual report. SIRC has three core responsibilities: to certify the CSIS director's annual report to the Minister of Public Safety, to conduct investigations into complaints from the public that happen from time to time, and to carry out in-depth reviews of CSIS activities. Simply put, SIRC is key in providing accountability to CSIS.

● (1115)

[*Translation*]

The issue of information sharing was thrust in the spotlight post 9/11 as greater integration became the new modus operandi of intelligence work. As such, information sharing has been, and remains, at the forefront of SIRC's review work. In fact, I would say this issue is an integral component of almost every review we undertake: whether through the lens of a review of a particular CSIS investigation, activity or program, in Canada or abroad, SIRC must invariably examine exchanges of information with domestic or foreign partners.

SIRC assesses these exchanges against a number of criteria. We ask ourselves the following questions.

First, did CSIS act in a manner that complies with Canada's laws and legal obligations? Second, did this exchange fall within the scope of the established framework for co-operation, such as a memorandum of understanding or a foreign arrangement? Third, was the information shared factually correct and did it accurately reflect the nature and extent of the threat? Fourth, what were the disclosure risks of sharing this information, and did CSIS take appropriate action to mitigate these risks? For example, did CSIS take into consideration the human rights records of the foreign agency? Finally, did CSIS collect and retain information only to the extent that was "strictly necessary"? My colleague spoke about this idea of "strictly necessary" earlier.

As a result of this work, SIRC has put forward a number of recommendations in recent years aimed at enhancing CSIS's information sharing practices. To give you an idea, with respect specifically to domestic partners, SIRC recommended that CSIS develop clearer and more robust overarching principles of co-operation with CSEC, that CSIS finalize the completion of sections of a memorandum of understanding with CBSA, and that it develop deconfliction guidelines and renegotiate a protocol with Global Affairs Canada, which is the new Department of Foreign Affairs.

[*English*]

Let me move to my second point. Consistent with our ongoing scrutiny of CSIS's information-sharing practices, this year SIRC committed to a review of SCISA to gain an understanding of SCISA's impact on CSIS's information sharing with domestic partners.

As part of this work, SIRC will review all exchanges of information involving CSIS that have taken place under the authority of SCISA. This will give us an appreciation of the nature and scope of these exchanges. More broadly, SIRC will seek to assess whether existing practices were altered by the new legislation and, if so, the direction of these changes.

SIRC also intends to examine CSIS's engagements with federal partners as they move forward with the implementation of SCISA. In this context, I will echo the views of others in underscoring the importance of putting in place a supporting framework, such as specific formalized agreements between and among the various government partners involved in exchange of information under SCISA.

You have heard from witnesses who have commented on the broad nature of the threshold for sharing contained in SCISA. On this point, SIRC is of the opinion that formalized agreements to address the finer points of what information will be shared, how it will be shared, and what safeguards are attached to the information once it is shared are especially important. For this reason, in our review we will be attentive to these formalized agreements, where much of the work of determining the precise balance of security and privacy concerns will inevitably take place.

Indeed, insofar as there is always a level of interpretation, an important emphasis must be on review as a safeguard against unreasonable exchanges. For that reason, the role of review bodies such as SIRC is essential in ensuring that the proper balance is maintained.

I should end by noting that our broad access to CSIS information is key to allowing us to review CSIS's exchanges of information with partners. As you may know, SIRC—and it's important to remember this—has the absolute authority to examine all information under CSIS's control, no matter how classified or sensitive, with the only exception of cabinet confidences. Therefore, SIRC can examine all information that is shared with CSIS and, equally, all information that is shared by CSIS to its partners.

● (1120)

[*Translation*]

There remain blind spots, however, and this brings me to my last point. Although SIRC has great powers to review CSIS, this ability does not extend beyond CSIS. This means that SIRC cannot assess the source, validity or reliability of the information provided to CSIS by its domestic partners, nor how CSIS information or advice is used by these partners. In short, SIRC cannot follow the thread of information to allow for a more comprehensive review of CSIS's interactions and exchanges with domestic partners. We have already outlined this in previous reports.

This limitation is compounded by two other interrelated issues, which we discussed in the context of debate surrounding the Anti-terrorism Act, 2015, and SCISA. Seventeen departments with a national security nexus, including CSIS, are listed in the legislation as the recipients of information sharing in respect "of activities that undermine the security of Canada".

The first issue is that of those 17 departments, only three—CSIS, CSE and the RCMP—are subject to a dedicated review body. There is no review mechanism to scrutinize the exchanges of information of the other 14 departments.

The second issue is that the three review bodies in question, namely, SIRC, the Office of the Communications Security Establishment Commissioner—my colleague's organization—and the Civilian Review and Complaints Commission for the RCMP, cannot carry out joint work as their legislation extends only to the respective organizations they review.

In fact, we can share some information on our results generally and on operating practices, but we cannot share information, even if our relationship is very close.

In the absence of a body with jurisdiction over the broader national security community, or to a lesser extent an ability for review bodies to work together, there will be clear accountability gaps regarding domestic information sharing.

As many have commented on, considerations of SCISA cannot be separated from an assessment of the strength of the safeguards in place to monitor the exchanges that take place under its authority.

● (1125)

[*English*]

Let me conclude by thanking you for your work on this matter. Bringing this forward in this place is important for everybody, I would say.

The government has made a firm commitment to enhancing accountability. There is no doubt, in my view, that information sharing within Canada's national security community should be subject to appropriate scrutiny. SIRC's work no doubt helps to further this goal.

With respect to SCISA, SIRC looks forward to communicating the results of its SCISA review when they are finalized. As I mentioned, we are in the process of doing that right now. At the same time, I will take the opportunity to affirm to the committee that information sharing has always been a priority for SIRC and that we will continue to be alive to issues of information sharing.

With my colleague, I will be happy to answer any questions you have.

Thank you, Mr. Chairman.

[*Translation*]

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

[*English*]

We now go to our last presentation and the Civilian Review and Complaints Commission for the RCMP.

Mr. Evans, would that be you?

Mr. Richard Evans (Senior Director, Operations, Civilian Review and Complaints Commission for the Royal Canadian Mounted Police): Thank you, Mr. Chair and members of the committee, for inviting us here today to discuss the Security of Canada Information Sharing Act and its implications for the RCMP and our commission.

In 2014, amendments to the RCMP Act resulted in the creation of the Civilian Review and Complaints Commission. While the previous RCMP Public Complaints Commission was largely reactive and driven by public complaints, the new commission has been given a broad mandate to oversee RCMP activities. The change most relevant to the question before this committee today is that the commission now has the ability to conduct systemic reviews of any RCMP activity to ensure it is being carried out in accordance with legislation, regulations, ministerial direction, or any policy, procedure, or guideline, without having a complaint from the public or linking it to member conduct.

With this new authority we are currently undertaking two such systemic reviews. The first, into workplace harassment within the RCMP, was initiated last year at the request of the Minister of Public Safety. The second, initiated by the commission chairperson, is into the RCMP's implementation of the relevant recommendations contained in the Report of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar. The commission's review on the latter is examining the RCMP's national security framework, including policies, training, and operational files, to determine whether they are consistent with Justice O'Connor's recommendations.

Specifically, the commission's review is examining six key areas: one, the centralization and coordination of RCMP national security activities; two, the RCMP's use of border lookouts; three, the role of the RCMP when Canadians are detained abroad; four, training of RCMP members in national security operations; five, RCMP information sharing with foreign entities; and six, RCMP domestic information-sharing practices.

Regarding the domestic information sharing, the commission is currently examining the adequacy, appropriateness, sufficiency, and clarity of RCMP policies, procedures, and guidelines as they pertain to domestic co-operation with federal agencies and departments involved in national security investigations. The goal is to measure their consistency with Justice O'Connor's recommendations, including screening information for relevance, reliability, accuracy, and privacy; the use of caveats; and that the RCMP is continuing to refine its policy of co-operating with other federal agencies or departments involved in national security investigations.

With regard to the Security of Canada Information Sharing Act, the commission is examining, as part of this ongoing review, what the RCMP has put in place to address its new information-sharing powers, such as record-keeping of disclosures under the act, and how that relates to Justice O'Connor's recommendations. For example, Justice O'Connor's report stressed that information-sharing agreements or arrangements pertaining to integrated national security operations should be reduced to writing. This is important, and the commission will be examining whether the RCMP adheres to this recommendation with respect to information sharing relating to the Security of Canada Information Sharing Act.

With that, we'd be happy to answer any questions.

Thank you.

● (1130)

The Chair: That's very good, very brief.

I need a speaking list.

I have Mr. Erskine-Smith for the first seven minutes.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks very much.

I first want to make sure I understand the current state of affairs.

The Privacy Commissioner has done a bit of a survey with respect to information sharing or SCISA. He has a report before Parliament. Five institutions have either collected or disclosed information, four institutions have received information on 52 occasions, and three institutions have disclosed information on 58 occasions. CSIS is one of the four bodies that has received information; I don't know how many times. To date that information sharing has not been reviewed, but SIRC plans to review it.

Is that correct?

Hon. Pierre Blais: We are in the process.

As you know, we plan every year. Right now we have over 12 in our research plan, but we have other specific requests by the minister. One of them is on SCISA. We hope it will be completed by the spring. It will be in our report because, as you know, we're reviewing, we're not—

Mr. Nathaniel Erskine-Smith: That's understood.

It might make sense, though, given the relatively modest number of times this has been used.... CSIS would never come to you and say, "Here is the information we received. Can you review it in a more timely manner to give Canadians assurance that the information is being shared properly and in accordance with the law?" That does not happen.

Hon. Pierre Blais: It's not necessarily the way it is.

Mr. Nathaniel Erskine-Smith: Fair enough.

Hon. Pierre Blais: We conduct our operation of the committee. We review the activities of CSIS. You don't necessarily come to us asking, "Well, could you look at this and that?" We do that on our own. We prefer to be on our own to decide what we look at.

Mr. Nathaniel Erskine-Smith: Fair enough. So too with the RCMP. You plan to review, but there has been no review at this time of the information that's been received by the RCMP under SCISA.

Mr. Richard Evans: I think the only distinction I would make is that ours is not a plan; it's actually under way.

Mr. Nathaniel Erskine-Smith: It's under way.

Mr. Richard Evans: We will be reporting, hopefully by the spring, on that. It's very actively under way. We've received all the information that we've requested from the RCMP. We hope to report, as I say, in the spring.

Mr. Nathaniel Erskine-Smith: It's not necessarily a comfortable state of affairs in some ways. We have two institutions that are at least subject to review and that are currently under review. We have 15 other institutions subject to the act. Thankfully, CSC has not shared information. We're safe there.

I know CBSA has both received and disclosed information. It's not subject to any review. Immigration, IRCC, has both received and disclosed information, and it's not subject to review. Global Affairs has disclosed information, and it's not subject to any review.

I guess my question is this: given that it's an inadequate state of affairs, in my view, going forward, how do you see the review bodies working together to establish that full review? We had professors Roach and Forcese before us to say that government information sharing should be matched with a full review of that information sharing, and they would worry if there's piecemeal review and then no review.

How do you see your offices perhaps working together, or the Office of the Privacy Commissioner working with your offices?

Hon. Pierre Blais: If I may just go back to my comments on the way it goes with the sharing of information right now, as I mentioned, there are some bilateral agreements between players most of the time.

For example, Global Affairs Canada has a protocol with CSIS, and they're in a process to review it. It's the same thing in place with many others. With CBSA, there is one that they're working on. It is because the exchange of information existed before the law. CSIS has been collecting information for 30 years. You can imagine that they go in many directions to gather information.

Now, speaking for our committee, we encourage CSIS to have specific agreements with the partners, in Canada and outside, for obvious reasons, as I am sure you would understand, to make sure it's done properly and that there's nothing that could fall through the cracks or is not within the law. That's why we do that.

● (1135)

Mr. Nathaniel Erskine-Smith: I'm sorry to cut you off, but I only have a couple of minutes left.

Is it fair to say, though, going forward, that fundamentally you're just reviewing CSIS in terms of its information sharing? Do you view the Privacy Commissioner as playing a role, then, in reviewing all information sharing under SCISA? If it's not through the Privacy Commissioner, how can we adequately review information sharing under SCISA?

Mr. Jean-Pierre Plouffe: Just to answer your first point with regard to the possibility for review bodies to carry out joint work, right now we can't do that, as noted by my colleague. We work in silos. This is not adequate.

I have stated in the past that it would be desirable to give the existing review bodies explicit authority to co-operate.

Mr. Nathaniel Erskine-Smith: But even there, we have three review bodies and we have 17 institutions. That's a great answer, but unless those three review bodies, working together, have the capacity to oversee all institutions that are recipient institutions and subject to the act, how do we adequately review SCISA?

Mr. Jean-Pierre Plouffe: With regard to the 14 institutions, as I said previously, in my view it's important that they be subject to expert review one way or the other, or the committee of parliamentarians could decide that they want to do that themselves. It's up to them to decide that, but I still believe they should be subject to expert review.

How do you do that? Again, it's for the government to decide whether it wants to create one super-agency, for example, or whether it wants to divide those 14 institutions among the existing review bodies or create other review bodies. For example, perhaps the CBSA could be reviewed by the CRCC because, with regard to function, there is something similar, and so on and so forth.

Also, I must add that I feel that if the government feels that a super-agency is not in order, at least we should have a coordinating committee of some sort—and this was suggested by my colleague Justice O'Connor 10 years ago—where all the heads of review agencies meet and discuss problems in common. The committee of parliamentarians would be a practical solution, because they would have to deal with one body and not with 14, 15, or 17 institutions. This is what I would suggest.

Mr. Richard Evans: I'll just add one comment. There is provision in our legislation that serves as a good example. We do have that authority to conduct joint reviews, hearings, and investigations, but our legislation stops short of allowing us to it with our federal partners. We do it extensively in the law enforcement context with our provincial partners. There is a provision in the RCMP Act that allows that, and it works.

Mr. Nathaniel Erskine-Smith: Thanks very much.

The Chair: Good. Thank you, Mr. Erskine-Smith.

We now move to Mr. Kelly for around seven minutes.

Mr. Pat Kelly (Calgary Rocky Ridge, CPC): Thank you, Mr. Chair.

I had the opportunity earlier in this Parliament to introduce a private member's motion that dealt with Canada Revenue Agency, which is one of the agencies within this. It was not related to national security, but one of the anecdotes that came up during my dealing with that motion was the damage that can be done to someone through the sharing of incorrect information. In that case the CRA had marked somebody as deceased. They then shared that information with other government agencies, and so in the process of bringing this person back to life, so to speak, with all of the various government agencies with which this woman had to interact, her damages and the issues she faced were compounded by the fact that the information had been shared with Service Canada and with other agencies.

I'd like to address my question to Mr. Evans. If the RCMP collects and shares inaccurate information about an individual, what are the procedures to correct that information? When you try to correct information that's incorrectly shared and audit the accuracy, how can you ensure that you don't end up reporting incorrect information back and forth to each other from one agency to another? That is what really happened in this one case I'm aware of with the CRA, and it started this snowball effect of continually trying to mark this person as deceased.

● (1140)

Mr. Richard Evans: There are a couple of ways I can answer the question. The first is to say that in our reviews of RCMP activities and the conduct of individuals and incidents, we use that to inform broader systemic issues, so we will also be looking at internal processes within the RCMP.

We're approximately 60 people in our organization, and the RCMP has roughly 30,000 employees, so it's impossible for us to look at individual files.

My point is that we spend a lot of time reviewing practices and procedures to ensure there is effective internal oversight of the RCMP itself. Part of the answer, I guess, would be that we're looking to make sure that somebody is verifying, especially for that type of sensitive information sharing, what types of policies and procedures are in place to make sure there is sufficient scrutiny, potentially centralized control, before it happens.

The second part is that disclosure of personal information in the scenario you have described is a matter for the Privacy Commissioner. That is an area that would have to be reported. That breach of personal information being shared would be reported to the Privacy Commissioner.

Mr. Pat Kelly: It wasn't so much a breach. It was inaccuracy. If the information had been accurate in her case, it would have been appropriate to share that information.

Hon. Pierre Blais: In the first place, that says that there was a problem, in this case inaccuracy, so it would have to be corrected by, I would say, anybody. Nobody should provide any inaccurate information in the first place.

It's not a problem of sharing. It's a problem of having accurate information in the first place.

Mr. Pat Kelly: Fair enough, but I don't think any of us has an expectation that an organization—for example, the RCMP—with 30,000 employees will never make a mistake. I don't think it's a reasonable starting position to say that we'll just be perfect and then we won't have a problem with sharing inaccurate information.

Currently, how do you fix the mistake of information that was shared that was inaccurate, and what ought to be the way we go about this if we're to improve?

Mr. Jean-Pierre Plouffe: If I may, I'll comment on your question.

I think maybe one way to do it would be to incorporate into the act a provision that any information that is not relevant, which is the threshold used presently in the act, should be destroyed. This is not built into the act right now. In my view, that's a problem.

For example, I'm looking at section 10 of the act, which talks about regulations that could be made by the Governor in Council. They have three ways to make regulations. I would add a fourth one, which should read “destruction of information that is not relevant”. If you have a built-in provision to the effect that if it's not relevant, it is to be destroyed within a certain time, I think you would avoid the problem you just raised.

We have that with regard to CSE right now, the body I'm reviewing. If the information doesn't meet the criteria set out in the National Defence Act, the information must be destroyed.

● (1145)

Mr. Richard Evans: I can say in the context of the RCMP that there are accountability mechanisms built in. If you're talking about the conduct of individuals who have either collected or inappropriately shared inaccurate information, and members of the public become aware of that, they can certainly make a complaint that would come to us. The RCMP itself has its own internal mechanisms to discipline members if it is done in a way that's negligent or if there is some misconduct involved. There are adequate measures to address that.

The first part of my answer was that we try to make sure that it doesn't happen in the first place by having better practices, some oversight internally to make sure those mistakes don't happen, but there are mechanisms built in to deal with the consequences as well.

Mr. Pat Kelly: I guess we never—

Hon. Pierre Blais: This is an important point: corroboration.

CSIS has been collecting a lot of information, as you know, for 30 years. We were even blamed for keeping it too long. They often use corroboration to know whether information is right or wrong. Having information that is not right is a problem in the first place.

You have mechanisms in any organization to make sure that information is correct. Sometimes corroboration, or having many sources regarding the same information, is a good practice, and improving practices would probably help any of those organizations. It exists at CSIS. It exists for us as well, but as was mentioned—

[*Translation*]

we are not immune

[*English*]

of a mistake. Everybody makes mistakes. It happens from time to time.

The Chair: Thank you, Mr. Kelly.

We now move to Mr. Blaikie.

Mr. Daniel Blaikie (Elmwood—Transcona, NDP): Thank you very much.

My first question I think is relatively straightforward, and it's for the review bodies that have already started looking into information sharing under SCISA.

We've heard that there are a handful of agencies that have either transmitted or received information under SCISA and that there have been only 50-some instances of this. I'm curious to know how that's recorded. How many Canadians could be covered under one of those acts of information sharing? Fifty-some shares sounds modest, but if the information of tens of thousands of Canadians counts as one of those shares.... I'm curious to know, when shares are recorded under SCISA, how many people, potentially, are covered by one share of information. Presumably it's not a one-to-one correlation so that the personal information of only 50-some Canadians has been exchanged under the authority of SCISA.

Mr. Richard Evans: From our perspective, the best answer I can give you is that I'll have to get back to you when our report comes out. We are literally just at the stage now of reviewing those files. You're right that it could be one to one. It could be all sorts of different types of information sharing. We're just at a very preliminary stage right now in terms my being able to answer that.

Mr. Daniel Blaikie: Okay.

Hon. Pierre Blais: It's the same for us. It looks bad, somehow, but as we mentioned, we're in the process of a review. Maybe we'll have some more information when we table our report later this year.

Mr. Daniel Blaikie: For now it would be up to agencies like CSIS and the RCMP to characterize their shares. If they tell you that they've shared 18 times, it's up to them to generate that output based on whatever the sharing was. There's actually no established rule for saying what constitutes a sharing of information. They could reveal the entire content of a database and call that one instance of sharing.

Hon. Pierre Blais: Remember that some arrangements, some MOUs and agreements, already exist between certain of those institutions. We recommend that you develop more agreements and probably put in place some guidance on that. We obviously need some guidance. You cannot say, “Well, bring all that.” You should mention how to manage that. It's done already in some instances, but not everywhere, as I mentioned in my document earlier.

● (1150)

Mr. Daniel Blaikie: Okay.

I want to return briefly to the conversation around the possibility of having one super-office, if you will, that reviews information sharing across government agencies. I respect that the government obviously will have to make a decision about exactly how they want to do that, but I wonder if you could comment, given your experience, on the pros and cons of going with that approach, versus continuing to have multiple review bodies working in collaboration, versus bringing all those functions for the various agencies under one office.

Hon. Pierre Blais: In the United States, just to give you a flavour, they have 71 inspectors general looking at different areas of national security. I think it's about how you put those people together and about the mechanism for co-operation. Speaking for myself, I could say that the creation of the new parliamentary committee will give some power to....

I don't want to comment too much on that. The bill is before the House of Commons right now, at the report stage, probably, or close to it. This committee, when it's in place, will be able to have a look and co-operate with us. I think all of us have offered our co-operation to the committee to look into all the matters, because the committee will not be limited. It will have access to all. It may be limited access; I don't know, but it will be for Parliament to decide. Probably it will be

[*Translation*]

a step in the right direction.

[*English*]

It will be a first step, and we will see later on how it develops. For us, you cannot ask us to.... We do our jobs. We try to co-operate. We did inform the ministers that we should probably have the means to “follow the thread”. It's in the air. The government expressed their views on that.

For us, the more we can co-operate, the better for the information and national security community, I would say. You should remember what we all have in common, that we all want to protect Canadians from any threats from inside or outside. It's a goal that we all have. We cover a little angle of that. We ourselves don't do the operations, but we make sure that the operations of CSIS are done within the law.

We're all on the same side. All of the organizations are on the same side, the side of protecting Canadians against threats to national security.

Mr. Daniel Blaikie: I think you mentioned in your presentation that one of the challenges, though, was not being able to chase down the information outside of the realm of CSIS. Do you think just simply expanding the scope of SIRC would be the way to do that, or do you think it would be having one office or creating a mandate for review bodies to work more collaboratively? What are the relative pros and cons? Is there something lost in having one office?

Mr. Jean-Pierre Plouffe: The short answer is in Justice O’Connor's report. He has studied in depth having one super-agency versus keeping the existing agencies as they are. As an example, with regard to CSE or the Office of the CSE commissioner, Justice O'Connor has stated that it should not be included in this so-called super-agency because of its uniqueness. As you know, CSE is the foreign intelligence agency, or the electronic agency, and it's unique in itself.

Having said that, I think if you go to Justice O'Connor's report, you will find several pages on the pros and cons. For example, with regard to CSE, as the commissioner, I have one agency to look after. Therefore, I can go in depth because I have only one agency to review. Let's say, for argument's sake, that I would have five, six, or 10 agencies to review; I have the impression that the reviews that I would be making would not be as thorough. There are pros and cons about this so-called super-agency versus more focused agencies. As I said, Justice O'Connor has studied the matter thoroughly.

● (1155)

Mr. J. William Galbraith (Executive Director, Office of the Communications Security Establishment Commissioner): Mr. Blaikie, you raised two elements. One is the sharing of information and how to review the sharing of information between government agencies. The other part is the ability of the expert review process to get in depth into the agencies, as the commissioner stated. However, there is the issue that's raised by SCISA of who would be best suited to review the information sharing that's going on. The survey that the Privacy Commissioner has done gives some indication, and as the commissioner mentioned, perhaps the committee of parliamentarians might be able to follow that, but two distinct....

I think there has been general agreement on the need for expert review. The Privacy Commissioner has stated that need, and I think the results of the existing review bodies, as the commissioner and others have described, demonstrate the positive results of expert review and the need for it.

Hon. Pierre Blais: This is a major point. We should remember that we need experts drilling down in detail to the factual elements, as we do. We have done that for 31 years now, in our case, and we have experts. I'm sorry—

The Chair: I need to move on, since we're almost at 10 minutes for Mr. Blaikie, but I'm sure you'll get an opportunity.

Go ahead, Mr. Saini, please.

Mr. Raj Saini (Kitchener Centre, Lib.): First of all, good morning everybody. Thank you very much for coming here.

I want to stay with the same theme, but I want to just ask your advice on something, or where you think things could be improved.

We know the process of gathering information has changed over the last 30 to 50 years. We're relying less on human sources and more on technological sources, and this question probably pertains more to Mr. Plouffe.

We're talking about information gathering, and Mr. Blais, in your opening comments you talked about having specific, detailed information-sharing agreements. When you have 17 government departments and 110 agencies that have the possibility to share information and you're sharing information among yourselves, there are going to be ambiguous points. Information is shared and information is collected and then it's going to be shared with another body, so that information is going to be stored in one area and it's going to be shared with another area. How do we determine—Mr. Plouffe, I know you highlighted this in your opening comments—how that information is to be stored and how it is to be disposed of, if that information is not required?

I know the RCMP often conducts search warrants and that in some cases the information that you derive from the search warrant may be sent off to another organization. In the end, that information may be determined to be not actionable or not relevant, so I'm wondering where the information is being stored right now. Maybe you can give us some guidance about that. Also, could you comment on how that information should be disposed of so that it's not residing in one place in perpetuity.

Mr. Jean-Pierre Plouffe: In our case, as I think I mentioned previously, if the information that is gathered by CSE doesn't meet the criteria set out in the National Defence Act, it will be destroyed. They cannot keep it.

Mr. Raj Saini: Is there a time frame for that?

Mr. Jean-Pierre Plouffe: Yes, there is.

Mr. Raj Saini: What's the time frame?

Mr. Jean-Pierre Plouffe: I'm not able to say, I guess.

Mr. J. William Galbraith: It depends on the type of information. If it relates to information with a privacy interest and if it is not essential, as the commissioner referred to in his opening remarks, it would be destroyed. It's an automated process because of the extent of the technology employed by CSE.

For classified information that is shared within government, there is a government security policy, and departments are required to store and handle classified information according to that policy as well. It is left for those agencies that are receiving classified information to decide whether it is reviewed and to verify that the information is stored and retained properly. There are departmental security officers whose role it is to look after that information once it's received in the various departments.

● (1200)

Hon. Pierre Blais: You should remember, sir, that a recent decision by the Federal Court, by Justice Noël, which you probably heard about, insisted on the notion of "strictly necessary". It was mentioned by my colleague. CSIS, for example, gathers information. As you mentioned, it has changed. Years ago, and I remember that, you had information on paper. Now it's electronic, and it has changed a lot. It's still there, but Justice Noël rendered a decision with regard to collection and retention, and the government decided not to appeal the decision.

Mr. Raj Saini: Was this the court case this fall?

Hon. Pierre Blais: Yes, it was recent.

Mr. Raj Saini: The judge's comments were about breaching their duty of candour. Is that it?

Hon. Pierre Blais: Absolutely. In this case—and we put this in our report, if you remember, last year in January when we reported on that—the question was whether "strictly necessary" should apply all the time. It's a complex notion, but at the same time it gives the indication that they have to review all the documents on a regular basis to make sure that they don't keep that data too long, or for a period that will not be considered strictly necessary.

This is in the law. It will take some time for the service to get rid of the information that was gathered that was not strictly necessary. This is the guidance that we have in our law.

Mr. Raj Saini: I just want to follow up on that. I'm glad you raised that point, because some comments were made by the executive director of CSIS, who says that now with the change of government in the United States they have to re-evaluate some of the information they share. Are there any comments on that?

Hon. Pierre Blais: Do you mean Mr. Coulombe, the director?

Mr. Raj Saini: No, I mean Mr. Doucet.

Hon. Pierre Blais: Oh, it's not the service. You said director of the service, but you mentioned the director of our organization.

Mr. Raj Saini: Yes. I think it's Mr. Doucet, is it not?

Hon. Pierre Blais: Okay, I'm sorry, because you said the service.

Mr. Raj Saini: Sorry; I mean SIRC.

Hon. Pierre Blais: Sorry; could you repeat that?

Mr. Raj Saini: Now with the change in government in the United States, and even within the Five Eyes alliance, my main concern is that when we're providing information and we have information-sharing agreements internally, there is some mechanism whereby we can control the information, but when we share the information internationally, what control do we have?

Hon. Pierre Blais: As was mentioned, we have agreements—and I'm not talking about us but about the service—nationally and internationally to share information. As you know, and I'm not the first to say this, Canada is, as the expression goes, a "net importer" of intelligence. This means that we need intelligence, which we receive from other countries. It's important for our security and the security of our partners, particularly the Five Eyes partners, as you mentioned.

We have an ongoing agreement. CSIS has ongoing agreements, and information is shared within those agreements. I cannot comment on specifics, obviously, as you know.

Mr. Raj Saini: No, that's fine.

Do I have more time? I'd like to share my time with Mr. Lightbound.

Mr. Joël Lightbound (Louis-Hébert, Lib.): I have a quick question touching on what you said about the judgment by Mr. Noël. Has CSIS actually destroyed the data that it obtained illegally?

Hon. Pierre Blais: That's a good question. I did explain that you cannot just push a "delete" button. It's not that simple. Sometimes, and I'll use an example, it's like having the whole phone book, and you need just one page. In a sense, now, to destroy the information that is not strictly necessary, they need to review a lot of information, so it's going to take months to do that.

We have a team right now. As you know, the minister, using one section of our law, asked us to review that and make sure that it will be done. We're in this process right now. From our limited resources, we have taken people to do that. We're in the process of doing that, but it's going to take months. It's not something that you can destroy that quickly.

Mr. Joël Lightbound: The court did not impose a deadline, though.

Hon. Pierre Blais: No, I don't think so.

The Chair: We'll now move to Mr. Jeneroux for five minutes, please.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Thank you, Mr. Chair, and thank you for being here today and to your staff for preparing today, as well.

Mr. Blais, you mentioned your ongoing review of SCISA. I'll get you to quickly talk about what your timeline is, and the context. Are you seeing witnesses as well?

● (1205)

Hon. Pierre Blais: Do you mean the time frame for our research?

Mr. Matt Jeneroux: Yes.

Hon. Pierre Blais: I cannot give you details right now, due to the fact that usually we plan our research for many years, but this research will be done this year. It's in process now, and I'm pretty sure it will be finished by the end of the fiscal year.

Unfortunately, the way we do that is we put that in our report to Parliament and to the minister; however, the minister gets it during the summer, and the House should be sitting when we file the report. This year the report was filed sometime in September.

Mr. Matt Jeneroux: I'm curious about whether you are doing a lot of the same stuff we're doing, because we're going to present our report to the minister as well, so I'm just making sure we're not duplicating a lot of this.

Hon. Pierre Blais: Do you know something? We are independent. Our committee decided to review the impact of this legislation on the work of CSIS. I say that because it's important to know that it's not the minister who tells us what to do. We decided, because we believed it was important to review it.

It happens that Parliament is also reviewing, but....

Mr. Matt Jeneroux: Okay. I just wanted to clarify.

I'll also just clarify that the minister doesn't tell us what to do either. We decided on our own as well.

Following up on some of the questions from my colleague Mr. Saini on the other side of the table, I've asked a few of the witnesses here about some of the information-sharing laws of our allies within the Five Eyes. It seems that some aren't too sure of what they are. I'm under the impression that you guys would know what they are, so if there are aspects of our allies' information-sharing laws that we should adopt and consider, could the three of you, the different agencies, comment on what those would be?

Mr. Jean-Pierre Plouffe: I think we are, with all due respect, wandering away a little bit from SCISA, but anyway.

With regard to CSE, CSE has arrangements, or MOUs, with the Five Eyes partners—that's evident—but again what is important in those arrangements and MOUs is the fact that CSE stressed the point to its partners that it cannot target Canadians or people in Canada.

I think the partners have to be aware of that, in our case. It's vital. If not, we have a problem, because the National Defence Act is very clear that CSE cannot target Canadians and cannot target people in Canada. Therefore, this is the main issue we share with our partners.

Mr. J. William Galbraith: I would add that the signals intelligence agencies have an agreement not to target each other's nationals and to respect the privacy laws of each of the five members. That's amongst the signals intelligence agencies.

Hon. Pierre Blais: For us, you should remember that in some areas when we look at protecting Canadians and the security of Canadians, foreign fighters are one example of Canadian people are travelling abroad in some area and, as you know, it's public. We discuss this matter in our report almost every year. Obviously, we don't have the same environment as my colleague, Mr. Plouffe, and in those cases we are very prudent in the way we share information among the partners.

However, it shows, nevertheless, the importance of having a strong and clear agreement about how we share this information, given the problems that happened in the past with sharing that information, particularly with other countries.

We are an importer. We need information, but we also provide some information. It's a give and take. It's important, and we follow that very carefully. We look at this every year. This is an important part of our review, and we discuss that in our report every year as well.

● (1210)

The Chair: Thank you very much.

We now move to Mr. Bratina, please, for five minutes.

Mr. Bob Bratina (Hamilton East—Stoney Creek, Lib.): In the public framework of SCISA, the following statement occurs:

> Reasonable expectation of privacy enshrined in the Charter may be subject to reasonable limits where necessary to achieve an important objective, and as long as the limits impair privacy rights as little as possible.

Could I ask you to comment on the impairment of privacy rights, Mr. Plouffe?

Mr. Jean-Pierre Plouffe: Are you quoting from Mr. Therrien?

Mr. Bob Bratina: No, from the framework published under the—

Mr. Jean-Pierre Plouffe: I guess at first blush what I would answer is that it is important and vital to have a balance between security measures on the one hand and the protection of the privacy of Canadians on the other hand. I know that this objective is not easily attained, but I think this is what it is all about. Security measures are important in our day and age, as we all know. It's vital for our country, but on the other hand, I don't think this should be detrimental to privacy rights.

Mr. Bob Bratina: We had the War Measures Act, which became the Emergencies Act. Has anyone in the group—and I'll start with you, Mr. Plouffe—reviewed it with the view of how it might affect any of the current protocols in the state of a declared war or any other overt emergency? Is there anything in the Emergencies Act that you are aware of that would even override the current protocols under which we're working?

Mr. Jean-Pierre Plouffe: To be very honest, I'm not....

Mr. Bob Bratina: It's something of a concern, because it has happened in the past that the rights of individuals have been usurped by so-called emergencies, so I was curious about that.

Hon. Pierre Blais: You should know that when some intrusion is made that would go against the Charter of Rights, for example, it cannot ever be done without the authorization of a judge. The judge will apply the law of the land and will not set aside everything.

He will look at whether it's necessary to allow breaching somehow some fundamental rights, and as I'm sure you know, section 1 of the Canadian Charter of Rights and Freedoms says particularly that. It says that this charter could be infringed, if it's necessary, in some particular case. We forget that from time to time, but it's the case.

CSIS works without warrants when they're not necessary, but there's always.... This is an important point. Nobody raises it often, but it's important to remember that they never intervene without a warrant, and we look into all those warrants. This is part of our job, I would say. It's a major point to track down those warrants to see whether they're acting within the law.

Mr. Bob Bratina: Mr. Evans, in the information that you deal with in relationship with the RCMP, is this a case of a daily review of files, or does somebody say, "Oh, Evans is on the phone"? How does your department work in terms—

Mr. Richard Evans: You mean in terms of exchanging information?

Mr. Bob Bratina: Yes.

Mr. Richard Evans: When we initiate an investigation resulting from a complaint from a member of the public, or the systemic one that we're doing, the first step is to write to the RCMP, and they're required under the legislation to provide us with all relevant material.

There is a fairly elaborate process within the RCMP Act for providing that material to us. There are provisions in there that the RCMP can withhold certain information. I could go into a fair bit of detail, but it's largely a very co-operative relationship. We receive the information that we deem is relevant; if the RCMP has any objections to it, then there's a process in there for us to discuss it and elevate it. If the RCMP claims privilege over material, then we have to establish that it's relevant and necessary. That's our standard.

I can tell you that we've never been there under the new legislation. We normally can work these things out in a co-operative manner. We'll respect the RCMP's identification of privileged material or sensitive material. We'll go see it on RCMP premises, as opposed to bringing it to ours. There's a fairly elaborate procedure, but I have to say the RCMP have been very co-operative in providing us with what we ask for.

● (1215)

Mr. Bob Bratina: It's good to hear. It always raises the question for review bodies when there's someone in another office: "I've got this; do I give this to Blais or do I give this to Plouffe or not?"

The Chair: I'm going to give the microphone to Mr. Kelly, because your five minutes are up, or even 10 minutes. You're over already, sir.

Mr. Pat Kelly: I'm going to return to where I was with my first question.

I think we had a good discussion. I heard plenty of emphasis on the necessity and the importance of accuracy, but I think we also had agreement that it's not a reasonable premise to start from that agencies can achieve a perfect state where mistakes are not made and inaccurate information is never shared.

I understand, Mr. Evans, that breach of privacy is a matter for the Privacy Commissioner to investigate, but if information is shared and you want to correct and update or take back or somehow deal with something that has been shared with another agency, what is the process? How do you do that? How do you improve on...?

It may not be clear that a breach has been made or that there are clear damages to somebody from a breach of privacy, but simply that a mistake has been made. Some information has been conveyed that shouldn't have been, or perhaps if it had been accurate information, it should have been, but it's been found to be inaccurate.

How do you update another agency and ensure that they are not then re-sharing or not keeping their file in good order?

Mr. Richard Evans: If I understand your question, it's simply a matter of the best practice. If we're looking at an RCMP file and we discover that some erroneous information has been provided to another agency, we'd certainly expect that information to be corrected. We have the authority to make recommendations to the RCMP.

It's a difficult scenario without knowing the specific context, but we have the ability to make recommendations. I would hope that the RCMP would have corrected this on their own initially. They certainly would be able to go after the information, pull it back, and make the corrections. If we did a review of a file and found that they didn't do that, we would certainly have the authority then to make the same recommendations.

Mr. Jean-Pierre Plouffe: If I could comment on this very point, you mentioned that if there's a breach of privacy, in essence it would be for the Privacy Commissioner to investigate, but I want to stress that with regard to CSE, under the law in my mandate, I have also a mandate to protect the privacy of Canadians.

Therefore, every time we conduct a review, this is part of my mandate. I have to investigate whether or not CSE activities are considered a breach of privacy. If it is the case, I have to inform both the Minister of National Defence and the Attorney General of Canada that they are acting illegally, in essence.

Mr. J. William Galbraith: If I could just add to that, Commissioner and Mr. Kelly, we review on a regular basis a privacy incident file that CSE maintains.

Mr. Jean-Pierre Plouffe: It's called the PIF.

Mr. J. William Galbraith: In that, there may be, for example, the issuance of a report that may have had a name wrong or a named Canadian, and the reports will be retracted and re-issued and an assessment made of whether or not any consequences would be expected from that. We're reviewing that on a regular basis.

● (1220)

Mr. Pat Kelly: Mr. Evans, what proportion of the complaints that you receive regarding RCMP conduct are privacy-based?

Mr. Richard Evans: It's relatively small, because there's a provision in our legislation that allows us to refer a complaint to another body if it would be more appropriately dealt with elsewhere. When we receive those types, we give them to the Privacy Commissioner or the Access to Information Commissioner as well.

Mr. Pat Kelly: Okay.

Do I have any time?

The Chair: Just a bit.

Mr. Pat Kelly: Then I'll ask Mr. Blais one final question.

We've heard about real-time oversight, but that real-time oversight of CSIS's activities is simply not a reasonable expectation. Given that—and I assume you agree with that position—how close in time are your oversight actions related to CSIS operations? If information was improperly collected or inaccurate information is collected and shared, how soon would you be able to catch it and correct it through your oversight activities?

Hon. Pierre Blais: It's interesting, your question, because our name in English is "review committee" and in French it's

[*Translation*]

Intelligence Oversight Committee.

[*English*]

It's not the same. It's been there for 31 years, and I know that the first day I was appointed, I said, "What is that? It's not surveillance. Surveillance is oversight?"

Just to mention this point, we try in our review to get as close as we can to the factual points that are raised. For example, if there is an issue that is in the public domain, we try to put a team in quickly to look into the matter, but we cannot, I would say for obvious reasons, oversee when there are operations. It would be against all the rules and even the capacity of CSIS.

At the same time, we understand that our report is a little bit delayed compared to when things happen. We should remember nevertheless that in our report we mention when we did it, when CSIS reacted, and what the reaction was to it, which is the best we can do.

Maybe the committee of parliamentarians will have a little bit of oversight. I don't know, but it's the best we can do.

The Chair: Thank you very much.

Mr. Long is next, please.

Mr. Wayne Long (Saint John—Rothesay, Lib.): Thank you, Chair.

Thanks to the witnesses today.

I read a very informative article this past week. It was entitled "Canada's spy services should be more accountable". In that article Michael Doucet was quoted a lot. Some of this may be covered, and I'll throw this out for you, Mr. Blais. I'll try to stay on topic so my colleague across the way doesn't have a coronary today.

Voices: Oh, oh!

Mr. Wayne Long: There are 17 government agencies that can share information, and then there are three—CSIS, the RCMP, and the CSE—that have independent review bodies. I quote:

> "Today nobody has the ability to look at those 17 organizations from a real perspective, that is, across all organizations," he said. The problem is not just the lack of review bodies, but the inability of these bodies to share information with each other. SIRC cannot cooperate with other bodies to review other agencies despite them sharing intelligence with CSIS. "In my opinion, it's a failing of the system...."

Can you elaborate on that and tell me if there's anything new you would do to change that?

Hon. Pierre Blais: You're quoting whom?

Mr. Wayne Long: I'm quoting Mr. Doucet.

Hon. Pierre Blais: You're talking about sharing information with other organizations—

Mr. Wayne Long: Yes.

Hon. Pierre Blais: —in Canada or elsewhere.

It remains important all the time. I precisely mentioned with my colleague Mr. Plouffe that the two organizations, CSIS and CSE, share information, but the two bodies that are looking at them cannot.

Mr. Wayne Long: Right.

Hon. Pierre Blais: This is a problem that is there.

● (1225)

Mr. Jean-Pierre Plouffe: Even if we are buddies.

Mr. Wayne Long: Right, yes.

Hon. Pierre Blais: We identified that to the government. The government is aware of that. It's complex. It's easy to see the problem, but the means to address it are complex.

As you know, they're looking at this. That's why there is a consultation process right now to review all of that by the government. We expressed our views on that. I speak for myself, but I think Jean-Pierre and I both agree, and our colleagues in the RCMP as well, that we need more co-operation to help us, but it's up to the government to make the decision on that and find the right way to do it, and there's no magic solution.

Mr. Jean-Pierre Plouffe: I have just one comment on this point. It is true that right now there is no explicit authority to co-operate, but there's no explicit prohibition either. Therefore, practically speaking, over the past five years my predecessors and I have provided 10 or more letters to SIRC referring to specific issues that have arisen in my review of CSE that have implicated CSIS. It just means that even if we don't have the explicit authority, there's a certain amount of co-operation that could be done, and we are doing it.

Mr. Wayne Long: Okay.

Mr. Blais, the next question I have for you is again on another article I read. It said that 80% of SIRC recommendations were implemented by CSIS. Again, I'm quoting Mr. Doucet. He believed that the recommendations should be non-binding. I'll just quote the article here, where he says:

> If we were at 100 per cent, it would be like your kid coming home with straight A's. My initial reaction would be: 'School's too easy.' We want to put out challenging and thoughtful recommendations, but at the end of the day... Coulombe at CSIS will see them and prioritize them as he sees fit.

Is there something wrong with that, when you're satisfied that only 80% of your recommendations...? Square that for me.

Hon. Pierre Blais: All of our recommendations are in our report, and what is in our report as well is the response by CSIS. Sometimes they agree and sometimes they do not totally agree. It depends when the operations allow them to.

To give you an example, you remember what happened last year? We made a recommendation that they should go to the Federal Court. They said, “No, we're not going to Federal Court.” What happened? Federal Court—

Mr. Wayne Long: Yes, that was on the metadata.

Hon. Pierre Blais: Finally, even though they didn't agree, we were successful.

Ms. Chantelle Bowers (Deputy Executive Director, Security Intelligence Review Committee): Can I add something very quickly?

It's true that there's the Thomson decision of the court that says that our recommendations are non-binding. However, we do have a tracking tool at SIRC for the recommendations we make to the service, and we take it very seriously. We follow up with that, and we do have that tracking mechanism.

Mr. Wayne Long: Okay, just—

Hon. Pierre Blais: We review that every three months.

Mr. Wayne Long: Another point I want to make is that obviously we're in a new era now. You used to identify individuals and collect data on them. Now we collect data and identify individuals. One of the comments Mr. Doucet made was that this was okay, as long as you were conscious of protecting security and privacy.

Again, from your perspective, do you feel we have the right balance there?

Hon. Pierre Blais: We should remember, as we mentioned, that years ago we were collecting documents like this, printing copies and so on. Now it's changing to electronics, and sometimes with electronics we cannot collect just one piece; sometimes we need to have a bulk of information to find out what we need from it.

This is the problem that we face with the metadata question. I think it will be there for a while, in the sense that my friend and I have to look into two agencies and scrutinize them to make sure they will not abuse that and take more information than they need. At the same time, we have to allow them to make sure that they gather the information. If they don't have the information, lives could be at stake and problems could arise in other ways. Sometimes we have to balance that.

It has to be looked at on a regular basis. We cannot say it's this way or that way. We will have to follow up. I'm very prudent on that personally. I said it's important to make sure that we protect individuals, but at the same time, we have to protect the large community as well. Sometimes we need to have a bulk of information and find out where it is.

Before, it was easier; now it's more difficult.

● (1230)

The Chair: Thank you very much.

Ms. Chantelle Bowers: Could I add very quickly to what the chairperson added?

The Chair: Sure.

Ms. Chantelle Bowers: When we are reviewing CSIS's activities, we want to make sure that they're complying with the law, the ministerial direction, and policy. That also includes the charter. That also includes making sure that the privacy rights are being addressed as well. When we're looking at it globally, we're reviewing all of CSIS's activities.

Mr. Wayne Long: Thank you.

The Chair: Thank you very much.

To finish off the formal part of our questions and answers, we have Mr. Blaikie for somewhere around three minutes.

Mr. Daniel Blaikie: Thanks.

SCISA is, obviously, relatively new on the scene, and your organizations would have experience reviewing information sharing prior to SCISA. In your opinion, did SCISA really address some concrete problems? I know that two of your organizations are currently conducting a review of SCISA. In your organizations' experience with information sharing prior to SCISA, were there problems that you saw in your reviews of information sharing, problems with the agencies that you were providing oversight for not being able to do their job well, which you see SCISA as potentially addressing?

Hon. Pierre Blais: I am speaking for my organization. We were in favour of sharing information because it's helpful for CSIS to know more and to be well prepared to face the challenge.

On the question, we should know that our organizations are accustomed to confidentiality. Some of those 17 departments are maybe less accustomed to work in a confidential context, so there's a risk sometimes of something falling through the cracks and being published, but in our case, we're accustomed to that. We've had confidential documents for 31 years. We know that; we know what it is.

CSIS gathers information very easily, and we do look into matters. Other organizations will have to get accustomed to it and be well prepared and well organized to treat this information to protect people's privacy.

Mr. Richard Evans: From the RCMP's perspective, the answer to your question is in the terms of reference of the review we're doing. Justice O'Connor's report is 10 years old, and the recommendations were made with respect to RCMP information sharing. As my colleague says, it's been going on. Information sharing is the lifeblood of law enforcement, and that's why we're looking into making sure that it's done in a way that's consistent with the law. Regardless of what rules are in place, that's going to be the yardstick that we're using to measure it, whether it's SCISA or the Privacy Act or anything else.

Mr. Jean-Pierre Plouffe: Since CSE has neither received nor shared information under that law, I don't have any additional comments to make, unfortunately.

Mr. Daniel Blaikie: Okay. I guess that's just what I'm trying to get at. In our review of this legislation, we've had other witnesses say SCISA was a solution looking for a problem, as it were. I'm trying to understand better what the problems were in information sharing. What kind of information wasn't able to be shared under existing authorities, such that SCISA is representing an improvement?

I don't want you to prejudge the outcome of your reports in terms of whether SCISA's working or not, but can you give a concrete example of a type of case—not a particular case—where attempts at information sharing were frustrated, and the security purposes of the agencies that you review were being hindered because they didn't have adequate authority under the previous regime prior to SCISA?

● (1235)

Hon. Pierre Blais: Well, in speaking for us, we will know more when we get to our report.

The Chair: I think that's probably the wiser route, given the fact that we're already at four minutes.

If there is some information on your reporting or investigations you can share with the committee to answer Mr. Blaikie's question, we'd be happy to receive that information. I think he's asked a very good question

Hon. Pierre Blais: Mr. Chair, would you suggest that we provide our report to the committee when it's done?

The Chair: That's a good interpretation of what I was saying.

Hon. Pierre Blais: Excuse me; my only question is technical. I just want to make sure. I will look at how it could be done. We remit the document to the minister, and the minister, I think, has the obligation to file it in the House. We'll make sure that we respect that.

The Chair: We wouldn't ask you to—

Hon. Pierre Blais: I don't want to be sued by your colleague, the Speaker of the House. You see my point. I just want to be prudent—

The Chair: Given the fact we're discussing the rules, we should follow the rules.

Ms. Chantelle Bowers: We'd be happy to come back once it's tabled.

The Chair: That's fantastic. Okay. Thank you very much.

We will now move on. Colleagues, we have a few people who haven't had a chance to ask a question. I want to make sure every parliamentarian has an opportunity to do so.

Mr. Lightbound, Mr. Bossio, and Mr. Erskine-Smith have indicated they still have a little bit of follow-up.

Mr. Bratina, I did cut you off. Did you want to follow up on your line of questioning?

Mr. Bob Bratina: I'll hear the other guys' questions.

The Chair: All right, let's do it that way.

Go ahead, Mr. Lightbound.

[*Translation*]

Mr. Joël Lightbound: Thank you, Mr. Chair.

First of all, I would like to thank the witnesses for being here with us today.

Obviously, SCISA deals with national security and activities that undermine the security of Canada. If I, as a citizen, witnesses an activity that risked undermining the security of Canada, my first instinct would not be to contact the Department of Health or the Department of Transport.

Mr. Blais, you talked previously about the national security community. Who is part of this community? Are the 17 institutions listed in schedule 3 of SCISA part of the community?

I can understand why the Department of Finance is one of the institutions that can send or disclose information, but I can't figure out why several organizations are in schedule 3 as recipients.

My question is for the representatives of the three organizations that are with us today.

Given your national security experience, where do these 17 institutions fit in with schedule 3 of SCISA?

Hon. Pierre Blais: We aren't the ones who decided which institutions would be in the schedule. However, I can say that these institutions share information one way or another.

For example, the role of the Canada Border Services Agency is different from what it was 15 or 20 years ago. Currently, the agency directly addresses the possibility that some foreigners are entering Canada, while representing a terrorism threat. The same is true of organized crime, and the Department of Finance has a role to play in that area. The Department of Transport must deal with potentially dangerous situations that occur on board airplanes and trains or in stations.

That is why the government decided to put all these institutions in schedule 3, even if the percentage of security information that they may provide is 2%, 10% or 80%. The government didn't want any department with security-related information to be left out. In fact, the government would be better equipped than I am to answer this question.

Here is my vision of things. We often receive information, and it may have taken a different route than through the police or CSIS. It may come from another department. I think that we wanted to ensure that all information will be shared.

At one point in France, there was a problem at customs. The people responsible for I don't know how many deaths at an establishment in France entered the country from Belgium. Information from border services hadn't been shared. If that information had been shared, one of those people might have been stopped.

In order to act, all the services involved must receive information from every possible source. That's the best answer I could give you on that, Mr. Lightbound.

● (1240)

Mr. Jean-Pierre Plouffe: I would like to provide some additional information.

Paragraph 2(a) of SCISA deals with activities that undermine the security of Canada. The passage reads as follows:

> (a) interference with the capability of the Government of Canada in relation to intelligence, defence, border operations, public safety, the administration of justice, diplomatic or consular relations, or the economic or financial stability of Canada;

I guess that's the reason for the 17 institutions. Each one has a role to play, based on the definition in that paragraph.

Mr. Joël Lightbound: Thank you.

Mr. Evans, do you want to add anything?

[*English*]

Mr. Richard Evans: Just to add from our perspective, I agree with my colleagues. You have to think of national security as more than counterterrorism. It does go quite broad.

With our review, it's not just going to be about information sharing under SCISA. It will be information sharing writ large. What that means is that there may even be more than the 17 that are listed where information has been shared. Our report will be made public, so you'll be able to see that. It might give you a better sense of the nature of the information we're talking about and how it touches on so many different areas.

[*Translation*]

Mr. Joël Lightbound: I asked because only three of the 17 institutions that receive information have an

[*English*]

expert review body.

[*Translation*]

One solution might be to reduce the number of agencies that receive information. I'm not sure if this has been tried already. In any event, I agree that the definition is very broad.

Thank you. That was my only question.

[*English*]

The Chair: Mr. Bossio, welcome to the committee.

Mr. Mike Bossio (Hastings—Lennox and Addington, Lib.): Thank you very much, Mr. Chair.

Thank you all for being here today.

I found this very intriguing and informative and I appreciate the opportunity of being here today. I follow along the similar line of questioning as Mr. Lightbound and Mr. Erskine-Smith.

It seems to me the biggest problem is information in isolation. How do you connect the dots? You have one piece of the puzzle of a very large picture; how do you validate and evaluate the value of the information that you're receiving and therefore the potential threat to the country? There's also the potential abuse of that information or the misuse of the information or the relevance of the information or the false or inaccurate information that's received, and then the destruction of that information.

In an ideal world, it would be great to be able to assign the 14 agencies—or, as Mr. Evans just indicated, it could be more departments that share information—to a related oversight agency or a new one. Ideally, you could take one individual from each one of those oversight agencies to be a part of a super-agency with resources to target the bigger picture. You'd have the microcosm that is focused on those specific areas and have a larger group to look at the big picture and the overall threat. Would you agree that this would be an ideal scenario?

Mr. Jean-Pierre Plouffe: In theory, we could argue that a super-agency would solve all the problems. In practice, and in the meantime, there are ways to improve the system, if I may use the expression. The way to do it is very simple. It's to give the review bodies an explicit authority to co-operate.

This is quite easy to do. The government could it. Then, if they do that, it will be quite easy afterwards to make joint investigations and share operational information that we cannot share right now.

Again, I come back to what I was saying previously: it's that in the meantime, it's very easy to create a coordinating committee among the existing review bodies so that we are more efficient and more open-minded.

Mr. Mike Bossio: But nobody is explicitly legislated or chartered with the sole purpose of connecting the dots.

Mr. Jean-Pierre Plouffe: Not to my knowledge.

Mr. Mike Bossio: That's what I'm saying. Even under your situation, it would be organic, on an as-needed basis.

I would argue that you need somebody whose job, whose focus, is connecting those dots, and who then has the legislative authority to request that information to connect those dots. Unfortunately, you have silos in all the departments. The natural instinct is to silo and protect the information. If it isn't legislated to share it, you know as well as I do that a lot aren't going to share it.

Mr. Jean-Pierre Plouffe: I cannot answer for the agencies. I suspect that, for example, that the CSE chief might appear before you, and this is the type of question I would suggest you ask her at the time. In the meantime, with regard to review bodies, I come back to the comments I made a few seconds ago. It's quite easy, if they want to improve the system as is, to improve it. This is the recommendation that the existing bodies are all making. We are unanimous in that direction. Give us explicit authority to co-operate. Let's create a coordinating committee in the meantime. It will be easier and more efficient to deal with the committee of parliamentarians that is about to be created. Let's be practical in the meantime, and let's be efficient.

● (1245)

[*Translation*]

Mr. Mike Bossio: Thank you, Mr. Plouffe.

[*English*]

The Chair: Did you get your answer, Mr. Bossio? Okay.

Mr. Erskine-Smith is next.

Mr. Nathaniel Erskine-Smith: I have some yes-or-no questions for the most part.

Mr. Plouffe, you mentioned the Privacy Commissioner's preference for necessity, as opposed to the relevance threshold.

Could the three of you answer whether you support the necessity threshold, yes or no?

Mr. Jean-Pierre Plouffe: I mentioned that already. I said I am in general agreement.

Mr. Nathaniel Erskine-Smith: Perfect.

For the other two?

Mr. Richard Evans: Yes.

Mr. Nathaniel Erskine-Smith: Mr. Blais, would you comment?

Hon. Pierre Blais: It's not for me to comment about it. The government will decide.

Mr. Nathaniel Erskine-Smith: Fair enough.

Hon. Pierre Blais: It will be no.

Mr. Nathaniel Erskine-Smith: We have testimony that the relevance standard was created for disclosing institutions, and it wasn't to change the mandate of the 17 recipient institutions. We have had some testimony that we ought to clarify in black and white that the recipient institutions have to operate within their mandate to avoid any confusion.

Would you agree with that recommendation, yes or no?

Mr. Jean-Pierre Plouffe: I would say so.

Hon. Pierre Blais: Excuse me; I missed the point.

Mr. Nathaniel Erskine-Smith: It's to clarify in black and white that for the recipient institutions, their mandates have not changed, and that CSIS remains subject to "strictly necessary" and must operate—

Hon. Pierre Blais: Yes.

Mr. Nathaniel Erskine-Smith: Fair enough.

Mr. Evans, would you like to comment?

Mr. Richard Evans: When I spoke of "relevant" and "necessary", I was talking about the relationship between the RCMP and our commission as opposed to the sharing of the RCMP.

Mr. Nathaniel Erskine-Smith: Then I'll get your answer differently for my first question.

Under SCISA, institutions can disclose information if it's relevant to the recipient institution's mandate. It does not change the recipient institution's mandate.

I have two questions. Should the recipient institution be subject to a necessity collection requirement, and should we clarify in black and white that SCISA has not changed their mandate, because there has been some confusion in the academic literature to this effect?

Mr. Richard Evans: I would agree with that.

Mr. Nathaniel Erskine-Smith: Perfect.

My last question is about the review bodies. This picks up on what Mr. Kelly was asking about with the reliability of information.

Whatever the review body structure is, whether it's the three of you working together or whether the Privacy Commissioner is reviewing those other 14 agencies and their information sharing, and until we establish a more perfect solution, is it important that we have these review bodies and that we give them the power to compel the deletion of information where we have concerns with the sharing of the information and the reliability of it?

Mr. Jean-Pierre Plouffe: You're talking about the review bodies?

Mr. Nathaniel Erskine-Smith: The review bodies of the 17 recipient agencies under SCISA. Should they have the power to compel the deletion of information where that information is found to be unreliable or improperly shared?

Mr. Jean-Pierre Plouffe: The law will apply. If the threshold is relevance, fine. If it's not relevant, it should be deleted. If the threshold is necessity, then it's a higher threshold. If it's not necessary, then it should be deleted.

Mr. Nathaniel Erskine-Smith: Should the review bodies have the power to compel the recipient 17 agencies to delete the information?

Mr. Jean-Pierre Plouffe: I don't think so. This is not within the mandate in my view of a review body.

Mr. Nathaniel Erskine-Smith: Okay.

Hon. Pierre Blais: The mandate should be reviewed at the same time. It's difficult to respond. It's too narrow, I would say, for me.

Mr. Nathaniel Erskine-Smith: The review bodies in your view should not have the mandate to—

Mr. Jean-Pierre Plouffe: The review body normally will ensure that the agency in question does not violate the law and respects the privacy of Canadians. This is the objective of a review body. It's not an oversight body. It's not a refined review. It's a post facto review.

● (1250)

Mr. Nathaniel Erskine-Smith: Right. In Mr. Kelly's case, if there's unreliable information and you have discovered that the RCMP has received unreliable information or otherwise shared unreliable information, should some body that is reviewing these 17 recipient institutions compel the deletion of that information? Should someone have the authority to do that?

Mr. Jean-Pierre Plouffe: I made a suggestion earlier on about the section that deals with regulations, which is section 10. I suggested with regard to the powers of the Governor In Council to make regulations that a fourth criterion should be added. It should read something like this: “The destruction of information that is not relevant”.

Mr. Nathaniel Erskine-Smith: Or if we change the threshold that it's not necessary.

Mr. Jean-Pierre Plouffe: Yes.

Mr. Richard Evans: I would like to add in the law enforcement context, which is an answer I wanted to provide to an earlier question as well, that there's another layer of complexity in the law enforcement when it's information that's obtained by virtue of a search warrant, because then you're getting into judicial authorization.

When law enforcement bodies obtain information pursuant to judicial authorization, they report back to the issuing authority, so it's out of their hands to destroy or handle that information in any way. It belongs to the judge who issued the search warrant. There's a different set of parameters in the law enforcement context.

Mr. Nathaniel Erskine-Smith: Mr. Lightbound asked about this at a previous committee meeting. To pick up on that, one example of why it's so important to clarify the mandate would be when the RCMP is required to obtain a warrant to receive information, but a disclosing institution provides that information and no warrant has been obtained. It would be to clarify that the RCMP does need to go off and obtain the warrant before they can receive the information and use the information. It would be good to have that in black and white.

Thanks very much.

The Chair: Thank you very much, colleagues.

I'd like to thank our witnesses for being here today. This was a very good discussion. I appreciate your patience with me as chair. We all got through this very well.

Thank you very much for your testimony. If we do need to follow up with you subsequently, prior to the filing of our report from this committee, we hope that you'll be able to provide any information that might be able to assist us. We thank you very much for that.

Thank you, colleagues. We'll see you in the House of Commons in about an hour.

The meeting is adjourned.