HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 035 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, November 22, 2016

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, November 22, 2016

● (1100)

[*English*]

The Chair (Mr. Blaine Calkins (Red Deer—Lacombe, CPC)): Good morning, colleagues. Winter has arrived and I see we've all managed to get here on time. Notwithstanding the cold temperatures outside, we'll have a nice warm friendly meeting here today, I'm sure.

We're going to continue with our study of the Security of Canada Information-Sharing Act, otherwise known as SCISA. We're privileged to have with us today, from the Office of the Privacy Commissioner of Canada, the Commissioner himself, Mr. Therrien, along with Ms. Kosseim and Mr. Morgan, who are no strangers to appearing before the committee. This is for the first hour of our committee meeting today. In the second hour we have another panel.

Colleagues, before we go any further, I want to say publicly, thank you very much, to Mr. Lightbound, one of the vice-chairs, who has filled in admirably in my absence for the last couple of weeks, as I have had to go to subcommittees of liaison and other things.

Mr. Lightbound, I really do appreciate it, so thank you very much.

Without further ado, Mr. Commissioner, if you would like to present your opening remarks, then we'll proceed to rounds of questions. Thank you for appearing today.

[*Translation*]

Mr. Daniel Therrien (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Thank you, Mr. Chair and members of the committee, for inviting me to discuss the Security of Canada Information Sharing Act, or SCISA, which was enacted under Bill C-51, the Anti-terrorism Act, 2015.

When Bill C-51 was introduced in Parliament in early 2015, I expressed strong reservations, which remain true today. In my remarks this morning, I'll briefly summarize these reservations and will then encourage you to review national security information sharing issues more broadly. Finally, I'll explain the review we have undertaken of how SCISA has operated so far and how other legal authorities are used by federal institutions to share information for national security purposes.

My first point is that the justification for SCISA should be made clearer. I recognize at a general level that greater information sharing may sometimes lead to the detection and suppression of security threats, but we have yet to hear a clear explanation, with practical examples, of how the previous law prevented the sharing of information needed for national security purposes. A clearer articulation of the problems with the past law would help define a proportionate solution.

Second, I remain concerned that SCISA authorizes information to be shared where it's merely relevant to national security goals. Setting such a low standard is a key reason why the risks to law-abiding citizens are excessive. If the necessity or strictly necessary criteria is adequate for CSIS to collect, analyze and retain information, as has been the case since its inception, it's unclear to us why this standard can't be adopted for all departments and agencies with a stake in national security. Necessity is the international privacy standard.

On a side note, the issue of standards leads me to the preamble of the act, which you discussed with government officials last week. This preamble indicates that information is to be shared among departments in a manner that is consistent with the charter and the protection of privacy. However, this is not a true legal standard, but rather a wish or a pious hope.

As we indicated in our submissions to Parliament last year, we believe that effective privacy protection requires more than guiding principles that don't have the force of law. It requires the adoption of real legal standards. The obligation to disclose information in a manner that is consistent with privacy protection should therefore become an enforceable legal standard, as is the case with the rules governing the disclosure of information. To that end, SCISA should adopt not only the principle of necessity, but also that of proportionality.

Third, independent review of information-sharing activities is incomplete, given that 14 of the 17 receiving institutions under SCISA don't have dedicated review bodies. A parliamentary review, such as the one suggested by Bill C-22, will help but is insufficient. All departments involved in national security also need to be reviewed by independent experts.

Fourth, retention rules should be clarified. If the government maintains that the sharing of information about ordinary citizens—such as travellers or taxpayers—is necessary to identify new threats, national security agencies should be required to dispose of that information after these analyses and when the vast majority of individuals have been cleared of any terrorist activities.

● (1105)

Fifth, the law should require written information agreements. Required elements to be addressed in these agreements should include the personal information being shared, the specific purposes for the sharing, and limitations on secondary use or onward transfer. Other measures should be prescribed by the regulations, such as safeguards, retention periods and accountability measures.

[*English*]

While SCISA was an important addition to the Canadian legal framework related to national security, it is intended to be one element of a much larger whole. Limiting your review to SCISA will give you a very incomplete picture of national security information-sharing activities. I would therefore encourage you to also examine information-sharing with international partners and domestic information-sharing under legal authorities other than SCISA. Knowing more about other authorities will give you a better insight into whether SCISA is really necessary.

When Bill C-51 was tabled, I committed to examining and reporting on how its implementation would ensure compliance with the Privacy Act and inform the public debate. Our findings following the first phase of our review of the first six months of SCISA implementation are tabled in the most recent annual report. We have identified a number of concerns and offered recommendations. The OPC has concluded that the privacy impact of the new authorities conferred by SCISA was not properly evaluated during implementation, and we recommended that formal privacy impact assessments be performed.

The OPC also found several weaknesses with a Public Safety Canada guidance document intended to help departments implement SCISA. Although Public Safety Canada agreed to improve the guidance, no changes have been made a year after the OPC provided recommendations aimed at minimizing privacy risks. During our review, the OPC sent a questionnaire to all federal institutions to determine how often SCISA was used and, more particularly, whether it had been used to share information about persons suspected of terrorist activities or about law-abiding citizens. Most institutions told us that they had not used SCISA during the review period, but that they relied, instead, on other authorities.

So, there is information sharing for national security purposes, but most institutions told us that they are relying on other sources of authority than SCISA.

Five institutions told us that they have used SCISA for a total of 58 disclosures and 52 receipts of information. Institutions also told us that all SCISA information-sharing activities in the first six months following implementation concerned persons suspected of terrorism.

During phase 2 of our audit, we will review departmental records to verify whether that information is accurate and whether information sharing under authorities other than SCISA concerned suspects or persons not suspected of terrorist activities.

The goal of this review is to provide as clear a picture as possible on the use of SCISA, and other laws, in order to inform public and parliamentary debate as we head toward the government's planned review of Bill C-51. We would like that review of Bill C-51 to occur with a clear, factual, evidentiary basis, as opposed to simply a discussion of principles, however important the principles are.

With that, I would be happy to take your questions.

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

We will now proceed to seven-minute rounds of questions, starting with Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): Good morning, Mr. Therrien, Mr. Morgan, and Ms. Kosseim.

It's always a pleasure to see you, Mr. Therrien and Ms. Kosseim.

Welcome, Mr. Morgan.

I want to ask you questions, because you've written about this before, and I've done my own readings. I want to talk to you about the information-sharing agreements, and specifically about something called “originator control”, which I'm sure you're familiar with.

Let's look at the 17 departments that are involved in information sharing. One of them is the Department of Health. By profession, I'm a pharmacist, so I want to stick specifically to this point. You have someone who collects information, whether they're medically capable or not—that's one issue—but in medicine, we do not use a necessity test. We use a relevance test, because we don't put that burden on the patient to have to tell us what they think is necessary. We take all the information.

If all the information comes to someone in that department and they are responsible for the subsequent use of that information, and it goes down to different departments, how do they know, further down, that the information they're divulging to other departments is relevant, necessary, or proportional?

● (1110)

Mr. Daniel Therrien: You're in the shoes of which person, then?

Mr. Raj Saini: I'm in the shoes of the Department of Health.

Mr. Daniel Therrien: Which is the sending institution or the—

Mr. Raj Saini: It's the sending institution.

Mr. Daniel Therrien: With the bill as stated, the sending institution would not know unless, as we're suggesting, there is an agreement between the sending institution and the receiving institution on the purposes for which the receiving institution will use the information, and there may be limits to other purposes. That's why the law, as it stands, is silent on this point. That's one of the reasons we think agreements would be helpful.

Mr. Raj Saini: Another issue is reciprocity. You expect that if there's an issue with some of the information being misused or divulged in the wrong way, that information, in the future, could be in peril.

I'm confused as to how we rationalize all this information that's going back and forth between different agencies when one agency may have a particular expertise and another agency may not have a particular expertise. That information is being shared, and then you have this reciprocal agreement whereby you're saying if you don't utilize the information properly then we will not send you information in the future. How does that all work? I'm confused.

Mr. Daniel Therrien: I think it takes a number of instruments. On your point that the sending institution may not be an expert, in the context of this legislation, on national security, that's quite correct. I think government envisions that before information is shared, there will be a discussion between the sending and receiving institutions as to whether, in the context of the current act, it is relevant to the mandate of the receiving institution, on which the first department may not be an expert, but the second is. There's a discussion about that.

Also, according to section 5 of SCISA as it is, the information has to relate to detection or suppression of national security threats. It may be that the sending institution is an expert, but it's more likely that the sending institution is not an expert and the receiving institution is.

It's the conversation between the two departments before the personal information is given by the sending to the receiving institution that I think will enlighten both parties as to whether the criteria of the legislation are met.

Mr. Raj Saini: One other point I'd like to raise is on the amount of information. As you can appreciate, we live in a world where a lot of information is collected. It may be disparate, or it may be disorganized, and you need people to process and analyze that information. Are you worried in some cases that we may be collecting and passing on too much information, and we may not be able to provide what is useful or discern what is relevant?

Mr. Daniel Therrien: Absolutely. There's a risk of that for intelligence-analysis purposes.

From my perspective, from a privacy-protection perspective, that is why you need a number of tools to ensure that information sharing occurs, because there is a value in information sharing for national security purposes, but you have to ensure that not too much information is shared and retained. It's through the sum total of the safeguards we propose that we think the risk of over-collection and over-retention will be minimized.

Mr. Raj Saini: How about the disposition of information?

If information is collected, retained, and analyzed, and it's found to be not pertinent or not relevant, what's your opinion on the disposition of that information? How should it be destroyed?

● (1115)

Mr. Daniel Therrien: I think there are at least two steps to this question.

The receiving institution must determine whether it has the authority to collect it, to receive it. It may be that the sending institution will send too much information to the receiving institution. I would suggest that there need to be clear rules, which do not currently exist under SCISA, which require the receiving institution to get rid of it ASAP because it doesn't have the authority to collect it. That's the first thing.

Then there will be situations in which the information may be relevant for the analysis to be performed by the receiving institution, say CSIS. The information will generally lean towards the vast majority of people about whom we receive information not being security threats. That's another step where, at that point, the information needs to be set aside. It was useful for analytical purposes initially, but the analysis has now taken place and the vast majority of people about whom information is shared are not security threats. It should be destroyed then as well.

Mr. Raj Saini: Do I have more time?

The Chair: You have 20 seconds.

Mr. Raj Saini: I have a larger question, but 20 seconds is not going to cover it.

The Chair: I think we'll have time to get back to you, Mr. Saini.

We'll now move to Mr. Kelly, for seven minutes, please.

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

Commissioner, I take it from your remarks that you have a sense of skepticism over the necessity of this act. Is that a correct characterization?

Mr. Daniel Therrien: What we're saying is that there were authorities, and they continue to be used. That's one of the things we found in our review of SCISA. There are many other lawful authorities for information sharing and national security that have been used in the past. What I'm saying in terms of necessity is that we have not seen a clear articulation with clear examples of how the previous law created an impediment to desirable information sharing. There's a discourse that information sharing is desirable from a national security perspective. I think that's correct. But there was no absence of legislation before SCISA. There were many authorities. What we've not seen is evidence that the previous law was insufficient or created impediments to the work of national security agencies.

Mr. Pat Kelly: What would you make of some of the testimony we heard last week when representatives of various institutions and agencies that fall under SCISA commented on a reluctance to share over liability or fear of being in breach of the Privacy Act? These are people who are in the business of keeping Canadians safe and of gathering information or enforcing the law, who are concerned and afraid about the enforcement of the Privacy Act and about erring, perhaps, on the side of not sharing rather than sharing.

Mr. Daniel Therrien: That may be, but I would say that at the end of the day, to argue that the previous law led to concerns about what authority officials had with regard to sharing goes to whether the previous law was sufficiently clear and well understood. It doesn't go to the necessity for a new law. If, previously, officials were unclear, then the officials should have received better guidance and information as to what the law provided. But if this law, SCISA, is really necessary, it should not be so on the basis that previously officials were unclear. That lack of clarity doesn't necessitate legislation. It would be on the basis that not only was it unclear, but it was insufficient, that it was an impediment, and we've not seen evidence of that.

Mr. Pat Kelly: Your initial audit, or questionnaire, if that's what it was, revealed that many institutions had not shared information using the provisions of SCISA, but had relied on.... Could you elaborate a bit on the other authorities that people would use, if not SCISA?

● (1120)

Mr. Daniel Therrien: We did not ask in our questionnaire what the other authorities were and how often they had been used, because we focused on SCISA. But we did ask whether they were using SCISA, and if so how often—hence the numbers we have—and whether they were using other authorities. We did not ask how often and which types.

We know that there are other authorities, such as the immigration act, the Customs Act, and at a more general level, the common law authority of the police in the course of investigations, to share information for the purpose of investigations, and the defence prerogative, which authorizes the defence department and the Canadian Armed Forces to share information for national security purposes. There is a whole list of other authorities that previously existed. I'm not surprised to see that these other authorities continue to be used. That's a fact. But I think knowing what these other authorities are, how often they are used, and what this means in terms of the necessity of this new piece of legislation should be part of your consideration.

Mr. Pat Kelly: Is it really a matter of what some are characterizing as a lowering of the bar for privacy under this act? Is it a necessity, and is that threshold your principal criticism?

Mr. Daniel Therrien: Do you mean whether it's a necessity in terms of maybe not being necessary for this legislation to be adopted at all, or as a threshold for transactions and information?

Mr. Pat Kelly: I mean as a threshold for transactions.

Mr. Daniel Therrien: I would say that, yes, it is our main concern. It is not our only concern, of course, but it is the issue that I relate most directly to the ultimate risk, which is, I think, the risk to law-abiding citizens.

Mr. Pat Kelly: Of course, we are rightly concerned with Canadians' privacy. It's the business of this committee, as well as of your office, to ensure that Canadians' privacy is rightly protected.

Canadians would also be rightly appalled to learn, as a result of an inquiry into a future catastrophic crime or terror event, that there had been meaningful knowledge or intelligence that could have prevented such a crime or such an act from taking place, and that an agency had been reluctant to share it out of fear of an act and penalties under an act.

It is very important, no matter what we recommend, that we bear in mind that Canadians expect our various institutions of law enforcement and intelligence gathering that share information with each other to do their jobs correctly.

Mr. Daniel Therrien: Absolutely. I'm not disputing that at all.

The question is whether the previous authorities were sufficient, whether this new legislation was necessary, and, regardless, whether there are appropriate safeguards to ensure that this worthwhile activity does not create risks beyond those that are necessary.

Again, I would point out the risk to law-abiding citizens, to taxpayers, to travellers. There's no rule at this point in this bill that says that after information has been analyzed with a view to detecting national security threats, as it should be—that for the vast majority, for 99.99% of the people, whose information is shared—it should be destroyed ASAP.

The Chair: Mr. Blaikie, go ahead for seven minutes, please.

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

Thanks for your presentation. That was helpful in terms of trying to understand the thrust of the bill.

I think we're all agreed that we're trying to find the right balance between the legitimate use of information in order to stop security threats and the respect for Canadians' private information.

The gist of some of the testimony we've heard so far, in my view anyway, is that a lot of the controls for this information sharing are matters of internal department policy. In some cases, there are written agreements between the departments.

I'm just trying to get at what in SCISA actually mandates oversight. What's in the law that says from time to time departments will be evaluated in terms of how they are conducting themselves with respect to information sharing under SCISA?

Is there anything that requires departments to go outside themselves, as it were, in order to be evaluated, or is that something that really only happens as a matter of internal departmental policy?

● (1125)

Mr. Daniel Therrien: It's the latter. There's nothing in SCISA that legally requires this type of review or analysis.

I can do a review, as I'm doing, on my own initiative. I can investigate complaints, if they are made. However, in this type of area, the people who may complain don't know what's happening, so it's unlikely that there will be complaints raised to my office.

Of course, there are other oversight bodies that can act. However, in terms of, as you put it, internal controls, governance mechanisms, they exist, but they are wholly administrative. There's no legal requirement to have them.

Mr. Daniel Blaikie: Is it fair to say then that the main problem—if there is one—with SCISA is that it establishes a very low threshold for information sharing and retention but doesn't actually provide for any external oversight in terms of departments interpreting their authorities under the act to receive that information, retain it, and use it?

Mr. Daniel Therrien: I will say yes, and I can expand that to say the law facilitates, as a legal matter, information sharing. The safeguards—and you say, the "controls", but I'll say the "safeguards"—to ensure that these activities are not excessive are administrative and not legally required for the most part.

Mr. Daniel Blaikie: How would it be if the department were using some of this information in a way that Canadians would think was inappropriate? Other than a leak coming from somewhere in the department, is there any way Canadians could expect to find out that this is going on, then, or would it have to be someone reporting, in an unauthorized way, information they have by virtue of working within that department? Are there any other ways that Canadians would come to know of abuses of information within a department?

Mr. Daniel Therrien: I'll repeat that there are no legally required controls. There is a reference in the preamble to SCISA that says, among other things, that information sharing should occur responsibly. That's advice given by Parliament to departments, and I'm sure this advice in the preamble will lead to certain actions within the public service. However, it's left completely to the public service to determine what kind of controls or governance structure they will put in place to live by this principle of responsible information sharing.

We don't need to be overly prescriptive, but I think there need to be some high-end controls, safeguards, and governance mechanisms to ensure that this broad authority given by Parliament is exercised responsibly.

Mr. Daniel Blaikie: How would you characterize the best possible oversight mechanism, one that respects the sensitivity of the information, obviously, that's being shared and used to fight threats to national security but nevertheless is something Canadians can trust to have teeth when it comes to ensuring that government is using that information responsibly and not keeping it longer than it needs to or should?

Mr. Daniel Therrien: It starts with the legislation itself, so I would say that the standard matters and rules around retention matter. It should not be for the bureaucracy to decide how long they are going to keep the information. There should be rules of law on this.

There should be a legal requirement to have agreements whereby you bring the general principles to something more down to earth—what kind of information will be shared for what purpose, etc. Some accountability mechanisms in these agreements would be helpful.

Review of the agreements by review bodies like me, like SIRC, and so on would be helpful, because that will put an expert lens on whether the agreements strike the right balance. It will inform the review bodies as to how to direct their case investigations further down the road.

● (1130)

Mr. Daniel Blaikie: We've heard in some cases that either making the information-sharing agreements public or even just knowing that there's a written agreement between international governments, and not just among departments, would pose a potential threat to national security. Do you think there is a way to have those agreements? Do they all have to be made public, or would it be sufficient to have, in some cases, either the Privacy Commissioner or SIRC or others say, without revealing the content of those agreements, "We are aware of them and we think these are adequate", and for Canadians to know that those review bodies have access to those written agreements? Do you think a mechanism like that in the most sensitive cases would be—

Mr. Daniel Therrien: The latter is certainly possible. I don't see why SIRC, the OPC, or other review bodies would not be able to see the complete text of agreements. There may be some cases in which certain provisions should not be disclosed to the public for reasons of undermining methods of operation, but, by and large, I think the agreements could be public, subject to few and limited exceptions.

Mr. Daniel Blaikie: Okay.

The Chair: Thank you, Mr. Blaikie.

We'll now move to Mr. Long to wrap up the seven-minute round. We'll move to five minutes after that.

Mr. Wayne Long (Saint John—Rothesay, Lib.): Thank you, Chair. It's good to see you back.

Thank you, Commissioner, Ms. Kosseim, and Mr. Morgan for coming today. The more you come, the more you can be part of our club. I think for five appearances you get a special status. You might be close.

I read a *National Post* article that was done on your report , in which you basically said that the federal government has scant regard for privacy rights when it comes to national security. In your report you state that SCISA opens a door to federal government surveillance.

Do you really feel that way? Can you comment on that?

Mr. Daniel Therrien: I feel there are insufficient safeguards in the legislation to prevent that kind of risk from materializing. I'm not saying that government officials involved in national security are in bad faith and are looking to do surveillance of the population, but the safeguards are insufficient.

It's not just a theoretical concern. We have seen cases in the recent past where there has been excessive, sometimes unlawful, collection or retention of information. Think of the report of the CSE commissioner who found that the CSE had disclosed metadata to other countries illegally. Think of the recent judgment by the Federal Court that found that CSIS had unlawfully retained the metadata of a large number of law-abiding individuals who are not threats to national security because CSIS felt it needed to keep that information for analytical purposes.

These are not theoretical risks. These are real things, real concerns. Do we want a country where the security service has a lot of information about most citizens with a view to detecting national security threats? Is that the country we want to live in?

We have seen real cases in which CSIS had in its bank of information the information about many people who did not represent a threat. Is that the country we want?

Mr. Wayne Long: No, it's not.

What would be the number one amendment you would make immediately? What would be the first thing you would do?

● (1135)

Mr. Daniel Therrien: I would start with a threshold, but review is also important. To me, in order to have the right balance, you need the right safeguards and the threshold. The issue of relevance versus necessity is very important, but you also need review of these activities by independent review bodies. It's the combination of the two that I think elevates the possibility of having a balanced system.

Mr. Wayne Long: The article I read was interesting. It said there were only two of 17 departments and agencies with power to collect that believed PIAs, privacy impact assessments, were necessary.

Can you comment on that? Was it alarming that only two of 17 departments actually thought the PIAs were necessary?

Mr. Daniel Therrien: It is alarming.

Mr. Wayne Long: How do you change that? There's obviously a culture. If only two of 17 departments felt they were necessary, there's a problem there.

Mr. Daniel Therrien: I heard Minister Goodale ask departments to pay attention to their obligations to assess the privacy risks of these activities. That is more encouraging, but to this day, we haven't seen the privacy impact assessments of these other institutions.

So, yes, it is alarming. I'm somewhat encouraged by what the minister said, but it has not translated into us receiving anything at this point.

Mr. Wayne Long: You haven't seen any substantial change?

Mr. Daniel Therrien: Have we ween any new PIAs? No.

Mr. Wayne Long: Also, in the paper, you criticized the tone of government's online consultation. There was a consultation paper that was asking for feedback. You didn't like the tone of it. How come?

Mr. Daniel Therrien: That consultation deals with the national security framework, writ large, way beyond SCISA.

I said a number of things. One, I think it makes a lot of sense to look at the framework as a whole and not focus on constituent parts. That's why I say I think you should look at information-sharing authorities beyond SCISA, because to have a real picture of what's going on, you need to look at the whole situation. So that is a positive aspect of the consultation.

What I did not like about the tone or the perspective was that you started an exercise with a view to reviewing and repealing potentially problematic elements of legislation that give additional powers to state officials, but the consultation paper in large part suggests further extensions of state powers as opposed to more privacy protection or more human rights protection.

I'm not saying that it's illegitimate or that it's not a good idea to look at the framework, writ large. It's a good idea, but the framework, writ large, should be looked at in a balanced way, such that, as it should be for SCISA, the new state power should be demonstrated to be necessary. As you look at these other issues, you should also look at what safeguards should be added or enhanced to create the right balance. The latter I did not see a whole lot of in the consultation paper.

Mr. Wayne Long: Thank you.

The Chair: Colleagues, do you mind if I take the five-minute round? Our party is a little thin here today, so is that okay with you?

I cleared it with him.

Thank you, Commissioner.

One of my questions I think might have been asked by my colleague Mr. Kelly. At the end of the day, it sounds to me as though there is a mishmash of lawful authorities and no orchestrated plan for the sharing of information among various departments and agencies. You said that there are a number of other authorities that government agencies are using outside of SCISA.

My question to you is, from a policy perspective at the national level, should all of these authorities be consolidated in one piece of legislation so that parliamentarians, lawmakers, judges, and law followers all have an easy, accessible source of legislation when it comes to the sharing of information?

● (1140)

Mr. Daniel Therrien: It would be difficult, but it's an interesting idea.

Among the sources of authority are common-law or non-statutory sources of information, including the common-law powers of the police to collect and share information for investigative purposes, and the defence prerogative under which the defence department collects information. These are non-statutory sources of authority that, by definition, exist outside of the statute that you're envisaging. It's not obvious how all of this would work, but it's an interesting idea.

What I would say that may be helpful is that in respect of the safeguards I'm suggesting for SCISA as a threshold of necessity and proportionality, and in respect of the requirement for agreements that create clearer rules, some accountability, and retention periods, there is no reason these safeguards could not be in a statute of general application that would apply to the sum total of the sources of authority. That might be one way to ensure that safeguards for the rights of Canadians apply regardless of whether SCISA , the Customs Act, some other piece of legislation, or the common law is used. That would be the most practical advice I could give you on that point, but it's an interesting suggestion.

The Chair: At the opening of your remarks, you offered up your suggestions as an opinion. Your opinion is a professional opinion, because privacy is your wheelhouse, your bailiwick. It's what you know and that's the way it should be.

When it comes to security, in the staffing of your office, do you have people with specific skill sets to deal with privacy as it relates specifically to terrorism and national security?

Mr. Daniel Therrien: We can always improve on any subject matter, but we certainly have, not all of our employees, but a number of employees with both subject-matter expertise and the security classification to undertake this work. We could improve.

Of course, I would say that since 9/11 and the increase in state powers that have an effect on privacy, the number of investigations or reviews or privacy impact assessments we perform in this area is increasing considerably, so the number of people with the right expertise is inherited from a past in which these issues were less prevalent from a privacy perspective.

I do think that we have a core of people with the right skill set, which could be improved, but we certainly have a certain capacity.

The Chair: Excellent.

In one of your answers to a previous question, you said 99.99% of people's information that is collected is not needed. I'm wondering where you got that number.

Mr. Daniel Therrien: Ultimately, it's not needed. What I'm saying here is that if you accept the view that security agencies need to collect information about people other than suspected terrorists, say travellers to a certain country, in order to identify new threats, if you accept that as a premise, the activity to be performed by the security agency would be to go through the information from all these travellers, the vast majority of whom are not security threats, with a view to doing analysis, correlating this information, and finding in the thousands of people whose information you have, the one, two, or three who may be security threats. So my premise is that out of the information on the thousands of travellers whose information is sent, only that of the two or three should be kept after it has been analyzed.

● (1145)

The Chair: I see. Thank you very much.

Mr. Erskine-Smith, go ahead for five minutes, please.

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

You mentioned to my colleague Mr. Long that one of the most important changes is the threshold. You've hit that over the head a number of times. To be fair, when the previous government introduced this bill, we had John Davies before us, and he said that in 2004 the Auditor General examined how departments and agencies worked together to investigate counter-threats, and then again in a follow-up report in 2009 the AG found that departments and agencies were not sharing intelligence information because of concerns over violating provisions of the Privacy Act or the charter, whether this concern was valid or not.

You and Professors Forcese and Roach, who were before us, proposed a necessity threshold as well. We had the departmental officials before us and they said, hang on a second, that would be problematic for us because the disclosing institutions, 100 or so agencies, don't have the expertise to determine necessity. Therefore, we want to make it easier for them to get the information out the door while keeping in mind that the recipient institutions must stick within their mandate.

If we're looking at amendments and trying to balance the concerns of the department, would a possible amendment be that disclosing institutions disclose relevant information, but recipient institutions are subject to a necessity standard? Would that help both sides to find a compromise there?

Mr. Daniel Therrien: I think it's a very worthwhile idea to explore.

Mr. Nathaniel Erskine-Smith: Okay, I'll take that.

Mr. Daniel Therrien: I think you were told by officials that section 5 deals with disclosure. It is true that it deals with disclosure, i.e. not receipt, but once the disclosure has occurred under the relevance test, there is nothing that says—certainly not explicitly anyway, and I think it would be extremely ambiguous at best—what a receiving institution should do.

CSIS, under its legislation, has a clear collection-test necessity. I'm less concerned about it, but I'm concerned about all the other receiving institutions that may not have that kind of test.

Mr. Nathaniel Erskine-Smith: Exactly. So when Professors Forcese and Roach say as one of their recommendations "to make crystal clear that receiving recipients must operate within their existing mandates and legal authorities and that agencies put in place protocols for ensuring the reliability of shared information, as per the Arar commission recommendations", I presume you would agree, but it might also make sense to go further. CSIS obviously has a necessity test built into its mandate in terms of receiving information, and it might be even better, when we look at the 17 recipient institutions, to actually subject all of them, in order to receive information, to prove the necessity of it to their mandate. Therefore we want to allow for the government's concern with respect to disclosing institutions. They're obviously not going to get into the nuts and bolts to understand necessity. They could be subject to proving relevance on disclosure, but recipient institutions wouldn't be required to show that it was necessary to their mandate.

Mr. Daniel Therrien: I think that would be helpful, provided that there would be a difference, there would be a misalignment of thresholds between the sending and the receiving institution, which would by definition mean that the receiving institution would receive too much.

And there needs to be a clear rule—

Mr. Nathaniel Erskine-Smith: —as to what they do with that excess of information.

Mr. Daniel Therrien: —that they need to destroy or dispose of that information.

Mr. Nathaniel Erskine-Smith: Absolutely.

Okay, I agree with you there. My final minute goes to the review of whether these powers are being exercised appropriately.

We had department officials before us last week, and the CBSA official mentioned that obviously CBSA does not have an expert review body and that your office would in fact be the appropriate review body for the sharing of information. If we don't have a super-SIRC type of body, does your office have the capacity to review the sharing of information with 17 agencies, or is the answer in fact to have a super-SIRC type of body?

Mr. Daniel Therrien: We have some experts, but we certainly do not have experts in sufficient numbers to credibly review the activities of all departments other than the three that have existing review bodies.

Mr. Nathaniel Erskine-Smith: I have one final question.

Would you support the recommendation of Forcese and Roach to match information powers with amendments that give independent review bodies review over all of the Government of Canada's information-sharing activities under the new act, as well as their recommendation that the body would have the power to compel deletion of unreliable information?

● (1150)

Mr. Daniel Therrien: I think all departments involved in national security should be the subject of independent review. Should it be one or several bodies? That's a mechanical issue of a certain importance, but my point is that all departments involved in national security should be the subject of expert independent review.

Mr. Nathaniel Erskine-Smith: Thanks very much.

The Chair: Thank you very much.

Go ahead, Mr. Kelly.

Mr. Pat Kelly: Thank you.

You've been clear that you prefer, it would seem, the various other authorities that authorize the sharing of information, as opposed to SCISA as it is.

Mr. Daniel Therrien: No. It's not a question of preference. Information sharing for national security makes sense. It's necessary as a concept. Before SCISA, we did not have an absence of legislation. There was legislation. It's not that I prefer the other legislation; I'm just saying that, before you legislate further, you should look at whether the previous legislation was sufficient.

Mr. Pat Kelly: To make sure I understand your position clearly, you believe that the previous authorities such as they existed, the various enabling acts of other institutions as well as common law, were sufficient to ensure that the correct sharing of information—

Mr. Daniel Therrien: I'm not even saying that. I'm saying that there were several authorities that authorized a considerable amount of information sharing. I think it is up to the government to demonstrate why this was insufficient. I haven't seen the evidence. I'm just saying there's an absence of evidence.

Mr. Pat Kelly: We heard some evidence at our last meeting that many people who work in intelligence gathering and law enforcement were concerned about the implications of the Privacy Act. Their concern, perhaps rightly, perhaps not, was that the Privacy Act may have trumped other authorities that they would otherwise have looked to historically to share information.

What would you recommend as the best way to ensure that the fear of violating the Privacy Act doesn't prevent an important disclosure or an important piece of sharing between intelligence gathering and law enforcement?

Mr. Daniel Therrien: I think the government should think hard about it.

Let's assume—and it is probably true—that there is fear among certain officials that they do not have the authority. I'll assume that. I'll accept that. I think the government then has two courses of action available to it. One, we, as the government, are going to explore whether there is validity to these fears or not. Does the law actually prevent information sharing? They have experts in government who can actually look into the question and determine if the fear is valid or not.

If it is valid, you ask, how is it that the previous law created impediments? Then you craft your legislation to address the real impediments, not the feared impediments.

Mr. Pat Kelly: The law is one side of it. There is also institutional culture—

Mr. Daniel Therrien: Yes.

Mr. Pat Kelly: —which you cannot expect to immediately change ever, in any situation, just by changing your law in Parliament. The behaviour of people who work on a day-to-day basis is not going to immediately change, no matter what you do with your law.

Mr. Daniel Therrien: If the issue is culture and fear, not substance—and that may well be, and it's all right—I'm suggesting to you that to address a cultural issue, legislation may not be the best solution. It may be guidance, information.... But there may be substance to this fear. Then the government should identify what the substance is and the legislation should address the substance.

The Chair: Are you good, Mr. Kelly?

Mr. Pat Kelly: Yes.

The Chair: It's good if you are, because we can get one more in.

Mr. Lightbound, go ahead, please.

[*Translation*]

Mr. Joël Lightbound (Louis-Hébert, Lib.): Thank you, Mr. Chair.

Mr. Therrien, I have two questions to ask you. I asked these questions last week when we met with representatives of different law enforcement and intelligence agencies.

I understand that a warrant from a judge is required when, for example, the RCMP wants to obtain certain information as part of an investigation of a suspect. However, the person has a reasonable expectation of privacy regarding the information since it's protected by the charter.

What happens when the information is disclosed voluntarily because it's relevant to the Security of Canada Information Sharing Act, but the institution would have otherwise needed to obtain a warrant to collect the information? I've tried to obtain an answer to the question, but until now not much light has been shed on the subject. I don't know whether my question is fundamentally clear.

● (1155)

Mr. Daniel Therrien: I think the question is clear.

I'll refer you to the recent Federal Court decision of Justice Noël in the case involving CSIS. In a section of the decision, Justice Noël mentioned that, since the adoption of Bill C-51, CSIS is now obtaining information from the Canada Revenue Agency that previously required a warrant. At this time, CSIS is obtaining the information without a warrant because the Security of Canada Information Sharing Act makes this activity possible. That's what we see in practice. Some cases used to require warrants, but they don't anymore.

From a legal standpoint, to answer your question, the issue of whether the information sharing involves interests protected by the charter needs to be reviewed on an individual basis. Sometimes it will be the case, but not always. When it's the case, an analysis pursuant to the charter would be necessary. We would need to identify the protections and check whether a reasonable search can be conducted within the meaning of the charter. In addition, very often—I would say in most cases—the information will not involve interests protected by sections 7 and 8.

Mr. Joël Lightbound: Okay.

My second question concerns the provision—I don't remember the section number but I think it's section 8—regarding the immunity granted when the information is disclosed in good faith. The answers we received last week indicated that the provision doesn't protect the crown and that it simply protects employees by granting them a certain level of immunity when they disclose information. Do you share the same interpretation of this provision?

Mr. Daniel Therrien: Do you mean the interpretation that the provision doesn't cover the crown?

Mr. Joël Lightbound: I mean the interpretation that the crown doesn't have immunity and could be targeted. For example, Maher Arar could have obtained compensation despite this provision.

Mr. Daniel Therrien: I don't have the answer to this question. We can get back to you later if you wish.

The issues regarding crown immunity and the impact of crown liability are somewhat complex.

Mr. Joël Lightbound: I would appreciate it, if you can do so.

Mr. Daniel Therrien: Okay.

[*English*]

The Chair: Yes, thank you very much. If you can, Mr. Therrien, that would be great.

We have one last one-minute question from Mr. Blaikie.

Colleagues, you all have a budget in front of you. After Mr. Blaikie's question, rather than suspending, we'll proceed right to approving the budget while the witnesses change. Then we'll hop right back into the rest of the committee.

Mr. Blaikie, go ahead.

Mr. Daniel Blaikie: I just want to use this last minute to serve notice of a motion that I trust will be in order.

> That the Standing Committee on Access to Information, Privacy and Ethics, pursuant to Standing Orders 108(2) and 108(3)(h)(vii), undertake a study of the Conflict of Interest Act and other initiatives which relate to the ethical standards of public office holders; that the witnesses invited to appear before the committee in relation to this study include Jon Dugal, Coordinator of Development and Events for the Liberal Party of Canada to testify about his role in the organization of private fundraising events involving Cabinet Ministers; and that the committee report its findings to the House of Commons.

That's a notice of motion.

The Chair: It's a notice of motion. Please send the text to the clerk.

If that's the case, then, Mr. Commissioner, we thank you very much for appearing today. It's very helpful as we go through SCISA.

Mr. Nathaniel Erskine-Smith: Mr. Chair, I have one follow-up question, since we have him before us.

The Chair: Be quick, please.

Mr. Nathaniel Erskine-Smith: I wasn't exactly clear.

We had the department before us last week. They said the collection authorities have not changed. Therefore, if, for example, the RCMP were seeking to receive information that would have required a warrant before SCISA, it would still be required to obtain a warrant and to accept the information through SCISA.

You mentioned, in response to Mr. Lightbound's question, that perhaps it wouldn't need to obtain a warrant now after SCISA. I just wondered if you could explain that a little bit more. It sounded contrary to what the department official said last week.

● (1200)

Mr. Daniel Therrien: If they said their collection authority has not changed, I would agree with that proposition. However, if we're talking about the RCMP, the RCMP has very broad authority under the common law to collect, share, and analyze information for investigative purposes. If the information is relevant to a criminal investigation and does not attract a charter interest, then I don't think a warrant is required.

There may be some cases in which section 7 or section 8 would be engaged, in which case additional safeguards would apply.

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

Thank you very much, Ms. Kosseim and Mr. Morgan, for being here today. We know you'll be able to come back at any point in time as we continue, at a very brisk pace, reviewing various items of importance. Thank you very much for your time today.

Colleagues, rather than suspending, the clerk has submitted a budget to you. While we await our new witnesses for the second half of the meeting, we have a budget that we need to adopt for this particular study. In order for the clerk to pay the witnesses and so on, we need to go through this formality.

Is there anything, Hugues, that you need to add?

Does anybody have any questions about the budget? It's fairly straightforward.

It's moved by Mr. Lightbound that we adopt the budget as presented.

Is there any discussion?

Mr. Blaikie.

Mr. Daniel Blaikie: I just want to ask a couple of questions.

I don't think I'm up on the conversation about this. Is this to bring people here, or is this for us to travel?

The Chair: This budget, as it's presented, has witness expenses for people to come here, a video conferencing expense for people out of the country, and miscellaneous expenses—which are outrageous, if we're paying $500 a meal for what we're getting. Is this what's really being billed to the—

The Clerk of the Committee (Mr. Hugues La Rue): That's what's being budgeted, but that's not what we're spending.

The Chair: Okay. The budget is $500 per meal. I don't think we're spending that.

The Clerk: No, It's not even close.

We can order better stuff, if you want.

The Chair: This is not a request for travel.

According to the way we operate, every committee study that we undertake has its own independent budget. They're automatically approved. Once we pass this, we don't have to go to a subcommittee. Only if we travel, do we need to go to the liaison committee.

Mr. Daniel Blaikie: I just didn't want to say yes to something without being clear.

The Chair: I hope that's clear. We're good.

All in favour?

(Motion agreed to)

The Chair: Now we can start doing some expenses.

Colleagues, Tamir Israel and Wesley Wark are with us.

Thank you very much, gentlemen, for your patience as we deliberated a very important budget. As you will find out, your expenses will now be covered for coming here today, if you had any. I thought it was going to be a no-brainer until Mr. Blaikie piped up, but it's all good.

We have Mr. Wesley Wark, visiting Professor at the Graduate School of Public and International Affairs, University of Ottawa; and from the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, we have Mr. Tamir Israel, who was recently before the committee.

Welcome, gentlemen. We have one hour. We will let each of you proceed for up to 10 minutes with opening remarks, and then we will proceed to rounds of questioning. I will just go in the order in which I have you here on the agenda.

Mr. Wark, the floor is yours.

Mr. Wesley Wark (Visiting Professor, Graduate School of Public and International Affairs, University of Ottawa, As an Individual): Thank you.

Chair and members of the committee, I am grateful for the opportunity to appear before you to provide some views on the Security of Canada Information Sharing Act, or SCISA, which is now embedded in Canadian law following the passage of Bill C-51, the omnibus anti-terrorism legislation introduced by the previous government in 2015.

C-51 provisions came into force, as you know, in August 2015. The Liberal Party promised to repeal the problematic elements of Bill C-51 and is currently engaged in the process of public consultations on elements of Canada's national security, but the government's plans with respect to any possible amendments to SCISA, in particular, have not been revealed.

SCISA appeared as part 1 of Bill C-51 in 2015. I was invited to appear before the Standing Committee on Public Safety and National Security on March 24, 2015 to testify on Bill C-51 as a whole. In my testimony, I divided the measures advanced in Bill C-51 into three baskets: first, those elements that can genuinely advance security capabilities in a reasonable and proportional way; second, those that do not advance our security capabilities or fail to maintain the vital security-rights balance; and third, those that, I think, deserve to be put on hold for deeper reflection.

In March 2015, I placed SCISA, or part 1 of C-51, in the first basket, of appropriate security enhancements. I also argued, and I quote myself, that SCISA "would greatly benefit from some detailed amendments...to bring greater clarity, heighten...efficacy, reduce... overbreadth, and bolster the security-rights balance." Despite considerable public criticism of SCISA, no amendments were made to the act before it was passed into law. Nothing that has come to my attention since the passage of SCISA in unaltered form changes my essential view—that SCISA can and should be amended.

In terms of advancing security capabilities, the purpose of SCISA is, presumably, to try to ensure appropriate information sharing through exhortation, through a broadening of the information-sharing regime to encompass a large number of listed entities, and to allow for expanded information sharing under an altered definition of "threat".

The committee has heard from eminent legal academics versed in national security matters, from a civil society actor, from the Canadian Civil Liberties Association, from government officials, and, earlier today, from the Privacy Commissioner of Canada. The perspective I offer is informed by my understanding of how intelligence and security systems regulate their information systems. I'm sorry if what follows sounds a little philosophical, but it has a practical point.

The specifics of SCISA need to be examined in the context of five guiding principles that should inform any effective information-sharing system for intelligence and security purposes within government. These principles have long been recognized and are as follows: the need to know, the need to share, the need to secure, the need to avoid information overload, and the need to be accountable. These needs shape an effective and reasonable information-sharing regime in a democratic system. They encompass lawful mandates as well as privacy and civil liberties protections. They are meant to interact to ensure balance between over-ingestion and under-ingestion of information. They are deceptively simple in the literal sense of their meaning, but not easy to operationalize as a package.

I want to just run through these five principles briefly.

The "need to know" principle refers to limits on information sharing that are shaped by the lawful mandates and operational needs of the agencies involved and by the requirements of information security. The more sensitive the information—the more that information might reveal details of intelligence sources and methods—the more intensively does the "need to know" principle come into play. "Need to know" can also be infected by non-operational imperatives, including bureaucratic politics, management styles, and personal proclivities on the part of officials working in the security and intelligence system. It is important that the "need to know" principle operate appropriately as a limiting factor, but it is equally important that the principle not be shaped by extraneous dynamics.

The "need to know" provisions in SCISA are generally weak and under-defined. Paragraph 4(e), under "Guiding principles", sets out in a very general way the authorized actors in the revamped information-sharing regime. Subsection 5(1) of SCISA posits a need to know based on the notion of relevance, again a very general and potentially overbroad measure.

While it would never be possible to strictly operationalize a "need to know" function, because to do so might be to hamstring any information-sharing regime, SCISA errs, in my view, on the side of unhelpful generalizations, compounded by the implication of subsection 5(2) that, once information sharing is set in motion, it can continue down an undetermined path of further disclosure.

● (1205)

One remedy to consider would be to import a version of the limitation set out for CSIS in its act in section 2, through the use of a strictly necessary yardstick for information sharing.

Justice Noël, in a recent Federal Court ruling on CSIS warrants and the retention of metadata, has reminded us of the historical context of that CSIS-limiting clause. As Justice Noël indicated, it may be time to review the strictures of the CSIS Act, but if the strictly necessary provisions of the act are deemed worthy of maintaining, then their applicability to an information-sharing regime for national security purposes seems, to me, obvious.

Then there is the need-to-share principle.

The need-to-share principle rules SCISA. This might be regarded as an "Oh, duh" moment, but the problem is that the principle rules in a completely unbalanced way that, among other problems, might have an impact on the very objective it seeks: more effective information sharing in the interests of national security. There are three problems, I think, with SCISA in its adopted form.

The first is the large number of entities listed for participation in SCISA's schedule 3. This list stretches the meaning of the core security and intelligence community to include many entities with only a very marginal role in national security matters. The list can be further shaped by Governor in Council orders that would not necessarily be in the public domain.

Many of the listed entities will be only bit players, at best, in the scheme. The recent annual report of the Privacy Commissioner gives substance to this reality, as he found that in the first five months of SCISA, only five institutions utilized powers in the act. A bigger problem is that while agencies outside the core security and intelligence community might on occasion have valuable information in their possession, they lack the attributes of rigour, methods, and understanding of national security matters.

The SCISA entities listed in schedule 3 should, in my view, include only core elements of the Canadian security and intelligence community. These can be identified and, in keeping with this, the list should be considerably reduced from the 17 named organizations. Moreover, I think there should be a requirement that all listed entities have a common formal memorandum of understanding to guide their information-sharing practices internally.

A second problem is the expansive justification for information sharing provided in SCISA. As noted, the justification found at subsection 5(1) is relevance, which is not, in my view, a tight enough criterion as it does not provide any rigorous guidance and does not allow for any real accountability. Relevance needs to be replaced by some form of language about necessity and should include a measure of proportionality that is linked to mandates and to threats.

The third and arguably the mother of all these problems is the question of how SCISA defines the nature of the information to be shared. SCISA adopts a new definition at section 2 regarding "activity that undermines the security of Canada", and I know you've heard a lot about that. This is a more expansive and open-ended definition than that provided in the CSIS Act, and I have heard no good argument for the change.

While I appreciate that the drafters of the legislation may have felt that a broader definition of the kinds of threats that now impact on Canada may have been required, on balance the definition they provided does not advance the public interest and has sown confusion and, in my view, many misplaced ideas about the powers provided for SCISA. A replacement use of the definition of threat in section 2 of the CSIS Act advances many of the same objectives, is an established criterion, and would provide greater clarity.

In particular, paragraph 2(i) of SCISA, as it currently stands, introduces a very dangerous dimension to government powers insofar as it opens the door to foreign interference in the domestic politics and sovereignty of Canada. It is also unclear to me how the SCISA definition of undermining the security of Canada operates for CSIS—one of the core agencies in the national security information-sharing regime—alongside its own mandate of threats to the security of Canada differently defined.

Fourth is the need to avoid information overload. Very briefly on this, one reason that it is important to find the right equilibrium between the competing demands of the need to know and the need to share involves the potential problem of information overload. If agencies and departments under SCISA are flooded with information that is ultimately not necessary to national security, not only does this information flood waste resources and personnel and impose additional burdens in terms of information security but it also hinders the overall operational effectiveness that is so important in a security and intelligence system that must constantly adjust its work according to its own calculations of threat and risk and that is always under immense resource constraints.

● (1210)

A too-expansive information system is not a precautionary measure; it can simply be an unnecessary burden. Too much information can be worse than too little.

The need to avoid the information-overload principle cannot be directly legislated. It has to be a product of the proper balance between need to know and need to share.

With regard to the need to secure, although SCISA contains an element of exhortation, particularly in sections 3 and 4, there is no exhortation regarding the related requirement in any information-sharing regime, and in particular in a more expansive system, for the careful protection of shared information. In an age of increased cyber-threats and in the face of the usual human proclivities for error and mishap, an expanded information-sharing regime must be accompanied by greater information-security practices. There is nothing of the sort in SCISA.

One way that such practices can be subject to internal self-examination in the departments and agencies involved in information-sharing is through mandated privacy impact assessments, but I note that in the 2015-16 annual report to Parliament by the Privacy Commissioner, only two of the 17 entities authorized to collect information under SCISA had deemed privacy impact assessments to be necessary. Even in those two cases, the privacy impact assessments, which under Treasury Board guidelines are meant to inform policies prior to their being fully implemented, were still being developed.

Another measure that could be considered in amendments to SCISA would be to provide an authorized role for departmental security officers in monitoring and reporting on information security measures.

● (1215)

The Chair: Mr. Wark, I hesitate to interrupt. We normally allow about 10 minutes for opening remarks, and we're at almost 12 now. Are you close?

Mr. Wesley Wark: I'm very close. I'm happy to discuss this in questions. The last principle is one that has also come to your attention, I'm sure; it's the accountability principle. How do you ensure that SCISA can be held properly accountable? My recommendation in that regard goes to the question of mandatory record-keeping, which is discretionary under SCISA at the moment. I also suggest that the government follow through on its transparency pledges by providing for an annual report by the Minister of Public Safety, documenting the uses of SCISA.

Thank you, Mr. Chair. Sorry I went over.

The Chair: That's no problem. We just want to make sure we have time for questions.

Mr. Israel, you're next.

Mr. Tamir Israel (Staff Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic): Thank you, Mr. Chair. I will try to keep my comments brief so that we do have time for full questions.

Thank you, as well, to the members of the committee and to you, Mr. Chair, for having me back here again.

My name is Tamir Israel. I am the staff lawyer with CIPPIC, the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic. CIPPIC is a public interest clinic based at the University of Ottawa's Centre for Law, Technology and Society in the Faculty of Law. Our mandate is to advance the public interest in policy debates arising at the intersection of law and technology.

We are pleased to have the opportunity to testify before you today on the study of the Security of Canada Information Sharing Act, which I will refer to as SCISA.

As you are aware, SCISA was introduced last year as a central component of Bill C-51. In CIPPIC's view, SCISA constituted one of the more problematic elements of that legislative initiative, and it remains so.

Participation in modern life requires Canadians to entrust ever-growing amounts of data to their government, including sensitive financial, health, and other information. Providing such information to the government does not mean, however, that Canadians sacrifice privacy interests in this data, nor should it.

Core and long-standing privacy concepts such as necessity and proportionality, concepts intended to facilitate threat identification and prevention in a tailored manner, are wholly absent from SCISA, raising the legitimate concern that its mechanisms will be used in a manner that is disproportionate and that impacts heavily on the privacy of Canadians who have done nothing wrong.

SCISA's challenges arise in part from the regime it establishes, but also in part from gaps in the pre-existing framework that it expands and in which it was inserted. I will touch on a few of these problems, addressing specifically the relevance standard, the definition of security threats, and the lack of safeguards, which are issues you've heard of already. I will try to provide additional context and propose some solutions as I go along, some from within SCISA itself and some comprising amendments to additional regimes that come from without.

In particular, while I don't go into it in detail in my comments here, you've heard from many witnesses, as well as from Professor Wark here that the need for an external expert review body is paramount to maintaining the overall proportionality of Canada's national security framework, and that's no less the case with respect to the operation of SCISA in general.

I'll begin with a discussion of the relevance standard. It is one of the two core limiting principles within SCISA's information-sharing apparatus. It is an over-broad standard that's insufficient. Relevance requires the presence of a reasonable basis on which to believe that the information in question relates to, in this instance, the mandate of a SCISA recipient's organization, and to activities that undermine the security of Canada.

Relevance is perhaps the lowest and least-defined legal evidentiary standard. While CIPPIC would hope that a court ultimately interpreting the relevance standard in SCISA, and taking into account constitutional jurisprudence, would impart into it considerations of immediacy and imminence, we are concerned that the standard will be used to justify generalized information sharing.

This is indeed precisely what occurred in the United States with the National Security Agency. In powers newly granted to the NSA in 2006, the relevance standard was inserted as a key limiter intended to ensure the powers in question were employed only in the context of specific and immediate investigations of security threats. This relevance standard, however, was used to expand the powers in question rather than to limit them. Specifically, relevance had been defined to mean any piece of information that may one day be relevant to an investigation, facilitating a domestic dragnet program that involved the wholesale collection of everyday domestic and international call records in the United States on a regular basis.

The reaction of the USA PATRIOT Act co-author, Jim Sensenbrenner, who is a congressman, upon discovering the scope of application arising from this relevance standard, following disclosures by former NSA contractor, Edward Snowden, is telling. I quote:

> “We had thought that the 2006 amendment, by putting the word 'relevant' in, was narrowing what the NSA could collect. Instead, the NSA convinced the Fisa court that the relevance clause was an expansive rather than contractive standard, and that's what brought about the metadata collection, which amounts to trillions of phone calls.”

While Canadian jurisprudence may well arrive at a different conclusion as to the definition of “relevance” in the context of SCISA, CIPPIC is concerned that there is insufficient guidance within the act as it is currently drafted to ensure it is applied in a proportionate and narrowly tailored manner.

● (1220)

On the other hand, we have yet to hear a compelling case for a general departure from the existing exceptions already embodied in the Privacy Act, which SCISA envisions. Under the Privacy Act, there are two existing operative exceptions that agencies can already rely upon when attempting to share threat-related information with other government agencies. Paragraph 8(2)(e) provides an upon-request exception permitting government agencies to share citizen information with investigative agencies, if asked to do so, for the purpose of carrying out a lawful investigation. In addition, paragraph 8(2)(m) allows proactive disclosure of personal information where the government institution believes the public interest in disclosure clearly outweighs any resulting invasion of privacy.

In the government consultation paper currently being discussed as well as in testimony before this committee, the argument is advanced that these exceptions are insufficient, primarily because agencies lacking a security mandate lack the expertise or incident-specific knowledge to fully utilize the information sharing permitted by these exceptions. This may be the case, but it is by no means clear how SCISA's adoption of a highly permissive and open-ended standard will remedy this.

On the one hand, non-security agencies receiving specific requests from security agencies for data under paragraph 8(2)(e) are able to rely on the requesting agency's guidance. On the other, agencies are no better placed to identify the relevance of specific items of information to unknown or unknowable security threats than they are to assess whether disclosure of such specific items will be in the public interest, as they are already permitted to do under paragraph 8 (2)(m). In any non-generalized context, the information being shared will need some specific quality inherently indicating its relation to a known threat for the exceptions to apply. Assessments of necessity and proportionality can occur as readily in such contexts as can assessments of relevance.

CIPPIC would therefore encourage two amendments to correct the existing potential overbreadth in SCISA. First, we would replace the relevance standard within the act with one of proportionality and necessity. Second, we would encourage, as we have in our previous appearance before you, an amendment to the Privacy Act that would adopt an overarching proportionality and necessity requirement that would apply across all government sharing practices, regardless of the specific Privacy Act exception under which they are occurring. This would, as we indicated in our previous testimony, apply to information sharing done under SCISA, as well.

The addition of an explicit necessity and proportionality obligation would create a more precise framework for information sharing than that currently embodied in paragraph 8(2)(e) and paragraph 8(2)(m), employing the known standards of necessity and proportionality, which agencies have experience employing in a national security context. Overlapping protection in both the Privacy Act and SCISA would permit the Privacy Commissioner of Canada to oversee protection-related information-sharing practices while allowing other oversight and review agencies to assess necessity and proportionality within the context of their respective mandates. Supplementing these changes, we would encourage training units within different government agencies, potentially within the existing ATIP infrastructure that most government agencies have, to have expertise so that in-house capabilities can be developed to identify threat-related data.

A little bit more briefly, the “undermining the security of Canada” standard is the other key limiter adopted by SCISA, and you've heard some of this from other witnesses. We would concur with the testimony of these other witnesses in raising concerns that this standard is excessively broad. To assist the committee in its assessment of this overbreadth, we would like to provide two examples of how this overbreadth can lead to disproportionate or undesirable information sharing in a few definite contexts.

Specifically, SCISA's definition of security includes cybersecurity and a broad definition of cybersecurity. A single cybersecurity incident, however, can implicate the private information of hundreds of thousands of Canadians. All data affected incidentally by such a cybersecurity incident could be relevant, and the underlying security breach could be viewed as relevant to activities that undermine the security of Canada and, hence, could be subject to exceptions in SCISA. Given this potential for over-sharing, other jurisdictions have sought to address cybersecurity in an explicit manner that is distinct from other investigative contexts, and that specifically addresses these issues.

● (1225)

Additionally, while SCISA excludes advocacy, protest, dissent, and artistic expression from its definition of security, CIPPIC remains concerned that SCISA's security concept remains sufficiently ambiguous to undermine core democratic functions. We have seen government agencies recently targeting journalists, for example, in attempts to identify potential sources attempting to uncover police corruption. We have also seen the targeting of indigenous activists, not on the basis of their participation in protests per se but on the basis that such participation potentially poses a criminal threat to aboriginal public order events.

It is not clear to us that the prevailing exemption for advocacy and protest would exclude SCISA's being leveraged in these contexts for the purpose of preventing interference with public order. We are aware that the opposite conclusion is also possible and that the exception put in place is overbroad and doesn't allow for information sharing, even in contexts where violence may be the issue, but we feel it is sufficiently ambiguous to allow for either interpretation, and that is an ongoing concern for us.

Finally, CIPPIC is concerned that SCISA will be used as an avenue to feed domestic Canadian data into the Five Eyes integrated infrastructure in an unintended and unanticipated manner. CSE is Canada's lead Five Eyes agency and is a legitimate recipient of personal information under SCISA. While the framework under which CSE and its Five Eyes agency partners operate is presented as nominally excluding or limiting the impact on Five Eyes residents, and the permissive powers and activities granted to these agencies presume these underlying conditions to exist, SCISA could undermine those presumptions by allowing another direct avenue for Canadian information to flow into this apparatus.

Turning briefly to the lack of safeguards in SCISA, CIPPIC joins other experts in voicing our concern at the prospect of the nearly limitless post-collection retention that SCISA may facilitate. The Federal Court recently issued, as Professor Wark just mentioned, a decision heavily criticizing CSIS for its ongoing retention of large amounts of Canadian metadata that was not identified as necessary to any security threat and indeed was explicitly identified as not necessary to the resolution of any security threat.

In our analysis, SCISA could be perceived as providing CSIS with a justification for long-term retention of similar data, were that data disclosed to it through SCISA's information-sharing mechanisms. But we also note, more importantly, that other agencies such as the RCMP and CSE lack any form of retention obligations. We would suggest that the remedying of this lack of retention obligation would be best achieved through overarching amendments to the Privacy Act that would apply across all of government and impose an overarching retention obligation.

In addition, other overarching safeguards that could be adopted within the Privacy Act could provide additional safeguards and a better framework for legitimate information within a modified and reduced SCISA. These safeguards could include the adoption of privacy impact assessments and a more robust enforcement of the Privacy Act.

Those are my opening comments for today. I would be pleased to take your questions.

Thank you.

● (1230)

The Chair: Thank you, Mr. Israel.

Mr. Massé.

[*Translation*]

Mr. Rémi Massé (Avignon—La Mitis—Matane—Matapédia, Lib.): Thank you, Mr. Chair.

I'll ask my questions in French. I'll address Professor Wark first.

You referred to the recent Federal Court ruling that the Canadian Security Intelligence Service illegally retained data for 10 years. The court criticized CSIS for retaining metadata that wasn't directly related to threats to the security of Canada.

The Federal Court decision specified that, in practice, CSIS no longer needs a warrant to obtain information from the Canada Revenue Agency following the enactment of the Security of Canada Information Sharing Act.

Can you explain why a warrant is no longer required to access the information? You referred to the reason, but I want to hear your comments on this subject in particular.

[*English*]

Mr. Wesley Wark: Thank you. It's an intriguing question. I may not be the best person to try to answer it. I think it is an important question. It was raised, if my memory serves me properly, with the Privacy Commissioner in the previous session.

The best I can do is to give you my quick understanding of this, which is that there is a distinction between an entity listed in SCISA possessing information, if possessed lawfully under provisions of its own mandate, and the flow of information through the SCISA system to the receiving institutions. My assumption about the question of where the warrant regime sits in SCISA is, in part, based on the analogy with part C of CSE's mandate for assistance to CSIS and other security and law enforcement agencies. In other words, if an entity in SCISA possesses information under its own lawful mandate, and it has the grounds, which according to the act are as overly broad as these grounds might be, to share that information with another entity, then the receiving entity—in this case, perhaps, CSIS or the RCMP—would be receiving that information under the lawful authority of the original collector. From its perspective, as long as those receiving agencies had an appropriate mandate to receive that information, then they wouldn't require a secondary warrant to acquire it.

It's a very complex scheme, and I think it feeds back into the suggestion you've heard from many of us who have testified on SCISA, that the problem is created by the nature of the principles underlying SCISA, their overbreadth, and in particular the definition under which the act is meant to operate.

[*Translation*]

Mr. Rémi Massé: Thank you, Professor Wark.

Mr. Israel, do you have anything to add?

[*English*]

Mr. Tamir Israel: Along those same lines, the Federal Court hinged its decision on the fact that CSIS is mandated to collect information lawfully only if it deems it necessary to address a threat to the security of Canada. As Professor Wark mentioned, if it received it through SCISA legitimately, then it now has legitimately received that information, and it doesn't need to rely on its authority within the CSIS Act, which already has a necessity limitation built into it. I think it's subject to interpretation either way, but SCISA could be seen as overturning that decision in a way that would allow CSIS to legitimately receive metadata, which it could not collect on its own footing, and to then retain it indefinitely.

[*Translation*]

Mr. Rémi Massé: I'll continue with you, Mr. Israel.

I was particularly interested in your opening remarks. In its 2015-16 annual report, the Privacy Commissioner indicated that the Security of Canada Information Sharing Act opens the door to federal government surveillance.

If you agree with this statement, can you explain how this legislation now opens the door to government surveillance?

● (1235)

[*English*]

Mr. Tamir Israel: The explicit provisions in SCISA allow for sharing only of information already collected, but because it provides a number of agencies with the impetus to begin to look for threat information, primarily on the front line, it may affect the manner in which they approach the information that they collect and retain, because that is now a new consideration they will be using in assessing their own information-sharing practices. At that stage, it could indirectly facilitate the additional collection of information.

When you're talking about the Government of Canada, which is an immense bloc, it's been compartmentalized with regard to the data it collects for good reason, because when you're dealing with the tax agency, you're not dealing within an investigative context, and you're sharing information with the government for tax-assessment purposes. When you're dealing with education insurance, you're not dealing with the government in an investigative context.

Historically, it's been addressed as separate, compartmentalized agencies with different types of information, with the exceptions for information sharing being very specific and targeted. If SCISA facilitates a more generalized information sharing—and I realize it hasn't to date, but it could, as these types of provisions have facilitated that in other jurisdictions—then that could be seen as our facilitating surveillance in a very direct sense, even though the information was already held by one government agency but maybe not by others.

Does that help?

[*Translation*]

Mr. Rémi Massé: Yes, exactly.

Mr. Wark, do you have any comments on the subject? In your opening remarks, you spoke of the need for balance between—I'll use your words here—"the need to know and the need to share."

Do you have anything to add?

[*English*]

Mr. Wesley Wark: Thank you.

I think the importance of maintaining a balance between need to know and need to share, which has been an ongoing tension in the entire western intelligence world since the 9/11 attacks, is of critical importance. The problem I see in SCISA is that the balance was never properly thought through, and certainly was not found in terms of the legislative language adopted.

In response to the particular question about whether SCISA was a kind of back door to authorizing new information-gathering and intelligence-gathering powers—and this is a concern that many people raised in the context of the original debate over Bill C-51—frankly, I don't see that in SCISA or even implicitly in its knock-on effects. It doesn't change, as I think you probably heard. Certainly other committees have heard from government officials that it doesn't change the actual mandates and lawful information-gathering activities of any of the agencies listed in SCISA. It is purely about information sharing. Information sharing may trigger—and this is my colleague Tamir's point—additional intelligence gathering and investigations by agencies that receive information, but that activity could occur only under their existing lawful mandates.

The Chair: Thank you very much for that.

We'll move to Mr. Kelly for seven minutes.

Mr. Pat Kelly: Thank you.

Maybe I'll ask Mr. Wark this question. We have heard much about the lowering of the thresholds and—according to some witnesses and, probably, members of the committee—the problematic definition, or idea, of making activity that undermines the security of Canada part of the threshold for sharing information. However, I think that if you were to ask many Canadians if a law enforcement agency or an intelligence-gathering body possessed intelligence about an activity that undermines the security of Canada, they would want to ensure that such information is appropriately shared. People don't want the security of Canada to be undermined.

Could you give the committee an example so that we can understand the context? What would be an activity that undermines the security of Canada but that ought not to be shared?

● (1240)

Mr. Wesley Wark: Thank you, Mr. Kelly. I appreciate the question.

I understand the underlying implications of it. I think that probably all the witnesses you've heard from—including me and, though I wouldn't want to speak on his behalf, Mr. Israel—share the same objective. In other words, we want to ensure that Canadian security and intelligence agencies are able to appropriately share information.

The thing that perhaps a member of the Canadian public interested in this question would not fully understand is the issue of why this particular broader definition is needed. As I said in my testimony, I have not heard a good reason for that. What I would encourage the committee to do is to line up the new definition of undermining the security of Canada and its various clauses with the section 2 definition under the CSIS Act, which is of long standing, that defines threats to the security of Canada. It has been operationalized over decades within the security and intelligence communities.

We have arrived—the this term was used recently, in previous testimony—at a kind of cultural understanding of how that works.

There is nothing in the existing section 2 definition of threats to the security of Canada that would be weak or insufficient in terms of allowing, from my perspective, the kind of information sharing that is necessary and appropriate to securing Canadians' safety. The problem, I think, that many of the witnesses you've heard from see with this broader definition is that it is simply too broad and, worse, unnecessary.

Mr. Pat Kelly: Okay.

I guess I'm asking the flip side of this question. If nobody had demonstrated the need to change and now that the act is there, what would be an example of an activity that would undermine the security of Canada that shouldn't be shared?

Mr. Wesley Wark: It's a good question, but I think what we're saying to you, Mr. Kelly, is that the answer is, unfortunately, "Who knows?" This is an inappropriate definition that does not advance the interests of the security and intelligence community in terms of operational effectiveness and that threatens that balance of need to know and need to share with information overload, which has all kinds of other knock-on implications.

Going through the list in section 2 of SCISA, where these various activities that undermine the security of Canada are listed, you see that they are broader and looser and baggier definitions that are unnecessary when lined up with section 2 of the CSIS Act. For the life of me, I don't understand why we did not stick with the definition in section 2 of the CSIS Act, which encompasses everything that needs to be encompassed and avoids ambiguity and problems introduced by this newer definition.

If the committee has heard from some government official that there was something inadequate in the section 2 definition in the CSIS Act, then that would be an interesting thing to pay attention to, but I am not aware that you have, or that the public safety committee has either.

Mr. Pat Kelly: In the interest of moving along, I'll turn it over.

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

Mr. Blaikie.

Mr. Daniel Blaikie: Thank you very much.

For me, the overriding theme of the look at SCISA is to try to strike that right balance between what government needs to be able to do to counter legitimate threats to national security and the assurance that Canadians have the right to privacy and can share information with government with the confidence that it's not going to be used or abused or come up in odd ways to haunt them years later.

What we hear from departmental officials often is that if we, for instance, use a necessity threshold for the sharing of information, then that information won't get shared in time, or it will damage their operations.

If we want to do justice to the various principles that Professor Wark enunciated in his presentation, what are the oversight mechanisms that you see? To me, that seems to be an essential part of the program. Especially in light of everything we've learned over the last number of years about Edward Snowden and others, getting a little window into how government operates in some cases with this information, it's hard for me to think that Canadians are going to have confidence to trust government with their information unless they know that there's some kind of independent oversight.

What are the mechanisms that you can imagine that would allow for the operational latitude that security needs—not that it wants, but that it needs in order to do its job properly—and also give Canadians confidence that there's someone looking over the shoulder of these organizations that are entrusted with that information and that they're not simply policing themselves?

● (1245)

Mr. Wesley Wark: Thank you, Mr. Blaikie. I had the pleasure, once upon a time, of meeting your father. I just wanted to say hello.

There are various mechanisms in place. We're in the business, as you all know, of reforming and thinking about reforming the system. But the place to start with regard to SCISA and making sure that the government can be held to account for how this scheme is operated, even if it's amended, has to be proper record keeping.

Unless there's a paper trail, a digital trail, we'll never be able to do any accountability, and the Privacy Commissioner has made this suggestion in his annual report. That's one thing.

There is an issue of ministerial accountability as well. I note that the public safety minister, in recent testimony to the public safety committee, on the back of the Privacy Commissioner's annual report, said he has sent a letter out to all his cabinet colleagues encouraging them to ensure that all of their departments involved in SCISA are maintaining proper privacy protections. That's a step, but on its own, I think, it's an inadequate step, important as it might be.

So there's record keeping and ministerial accountability. Again, I would come back to the importance, certainly for the broader Canadian public, of transparency provisions that are part of the legislation. There is a mandated requirement to provide an annual public report from the relevant minister, in this case probably the public safety minister, on the operations of SCISA. It should be a meaningful report.

Then finally, there's the question of agents of Parliament and independent review bodies. Agents of Parliament, such as the Privacy Commissioner, clearly have a role to play. The Privacy Commissioner was trying to indicate that he has some resources but perhaps not enough. I know the Privacy Commissioner's office well. It's not my place to speak to it, but it has very limited resources on the national security side.

With regard to independent review, as everyone will know, the problem is that we don't have an all-encompassing independent review system. We have these siloed mechanisms that independently deal with CSIS, are meant to deal with the RCMP on the national security side but haven't yet, and deal with CSE, yet there's nothing for CBSA and many of the other core security and intelligence systems.

I think we're all at the point where we recognize that the system of independent review, which we've inherited over the years, is a legacy system that's not functioning well, and there are various proposals on the table for how to change it.

On top of that, a new committee of parliamentarians, if Bill C-22 is passed in Parliament, will be an added element in that picture of accountability.

Mr. Tamir Israel: In addition to everything Professor Wark just said, I would add that I think there are ways to improve the timing of assessments on necessity and proportionality, if those were adopted, and those would involve, I think, better training in government agencies that are going to be the recipients of these requests and that are not inherently national security agencies. You could train people within these agencies to identify this information or to become more familiarized with the standards that are required to make those assessments.

Necessity and proportionality are both very core operative principles that are used all the time in this context. They're not new ones that are just imposed here at random. They're the ones that CSIS currently operates under, as we heard, and they're the ones that other agencies operate under regularly.

Imposing those standards does not really limit the ability of the existing agencies to get information that they're not already getting —and we haven't heard that they're not getting enough information —but with sufficient training and resources, maybe you can get around the issues related to timing.

In addition, one of the outstanding recommendations from Commissioner Major of the Air India commission was to have a centralized national security entity to address information flows between security and policing and other types of agencies, and to have that type of entity or another agency, such as the Privacy Commissioner for Canada, with a better resource and more expansive mandate or a more expanded expert review body with additional operational capabilities, take a more active role in interacting with government agencies and helping them to make assessments around whether specific items of information are or are not necessary to achieve threats. I think having that type of capacity within government or within an entity within government to facilitate that type of information flow could address any of the timing concerns while maintaining the privacy standard that should be kept.

● (1250)

The Vice-Chair (Mr. Joël Lightbound (Louis-Hébert, Lib.)): You have 25 seconds.

Mr. Daniel Blaikie: Do you think for the oversight committee proposed in Bill C-22, it hurts the credibility of that committee as an oversight organization that government is able to censure what information committee members will receive?

Mr. Wesley Wark: I should say to the committee that I have testified on Bill C-22 in front of the other committee. To make a long story short, I think there could be some useful amendments to kind of restrict the powers of the government on a discretionary basis and to impose restrictions on information that could be accessed and information that could be reported on by the committee.

That said, even with no amendments to Bill C-22, I think it's a great start and long overdue, but I'm hoping there will be some amendments of that kind.

The Vice-Chair (Mr. Joël Lightbound): Do you have a quick answer, Mr. Israel?

Mr. Tamir Israel: Yes. I agree that the restrictions on the information it can receive and the information it can impart are both too restrictive and too much at the discretion of government. I think at the very least having an objective decision-maker weigh in on those decisions would be a great start in encouraging its independence as an oversight entity.

[*Translation*]

The Vice-Chair (Mr. Joël Lightbound): Thank you.

We'll now move on to the last seven-minute question period. We'll start with Mr. Bratina.

[*English*]

Mr. Bob Bratina (Hamilton East—Stoney Creek, Lib.): Thank you.

On the notion of retention of data, I'm assuming most data now is electronic in nature and is not in brown paper envelopes although even if it were, it would get transferred.

Then, apparently, 400-pound guys in their basement can access any information anywhere and we've seen the fiasco south of the border recently with regard to that.

My first question is how do you wipe information? How do you get rid of it?

Mr. Tamir Israel: There are ways to delete information securely. Even a preliminary deletion will eventually lead to the information being deleted, but you can more comprehensively take active steps to delete information, to wipe hard drives, and to insert random data over where the data used to be to make that more concrete.

I think what's really missing, though, right now is the impetus to delete information, because there is no retention requirement, as we've heard. It's easier to keep it forever and even with just the vague prospect of its utility down the road, even if it's a 0.001% chance, the impetus tends to be to retain it just because it is so cheap to do so.

One of the problems with SCISA is that the more the information gets spread around different agencies, the more we have the potential for it to be accessed by a third party one way or another. Again, a retention limitation would facilitate the security concerns as well.

Mr. Bob Bratina: Okay.

On the notion of parliamentary oversight, then you have government discretion as to whether the oversight body gets to see it or not.

Professor Wark, I will ask you this. Who is in the inner sanctum of the final decision as to...? To me, parliamentary oversight means at least the public has elected officials as part of the process, and that's the reassurance we have that the people are doing the right thing. Then there's discretion as to what information they get. Where does that sit—with whom?

Mr. Wesley Wark: Mr. Bratina, under Bill C-22, the ultimate discretionary authority-holder is the Prime Minister, and the proposed national security and intelligence committee of parliamentarians would be beholden to the Prime Minister in certain instances with regard to the information they can access and information they can report on. Again, I think many people who commented on Bill C-22 believe that it's perhaps over-broadly written and that it could be narrowed in terms of those restrictions. But it's important to say that the essential dilemma of parliamentary scrutiny of intelligence and security revolves around secrecy, and the need to both access secrets, in order to make sense of the security and intelligence world, and to protect secrets in the interests of Canadian national security. Bill C-22 legislation tries to find a fix to that difficult dilemma.

If I can come back just for a minute to your question about retention, it's absolutely true that most information these days is digitally maintained. There are still a lot of paper records around, particularly on higher-level decisions, memoranda to cabinet, and that kind of thing. But I would disagree with my colleague Tamir about the fact that there are no retention schedules. There are plenty of retention schedules. The problem is that they are not legislated and they're not available in the public domain, but the mechanism that is used to enforce retention schedules is ministerial directives to the agencies of the security and intelligence community.

One of the things I have pressed for in various circumstances, including with regard to CSE, is that some of those ministerial directives around retention of information could be made public without endangering national security to reassure the Canadian public that information is not being kept in an abusive and overly long way. The retention mechanisms do exist; they just are, unfortunately, and perhaps in some cases necessarily, secret.

● (1255)

Mr. Tamir Israel: Very briefly about that, the independent arbitrator for Bill C-22 on disagreements, some, including us, have called for a mechanism to allow disagreements to be referred to the Federal Court. The Federal Court has expertise in making these decisions.

Just very briefly, yes, absolutely, some agencies have retention limitations on an ad hoc basis that apply to certain subsets of information they collect, but an overarching retention limitation in the Privacy Act would provide for a more principled and across-the-board process. CSE has some retention limitations that are imposed on it, depending on the type of data it's collecting; CSIS doesn't have any, or didn't until recently; and the RCMP does not have many. It's very ad hoc now, and imposing an overarching principled retention limitation with the Privacy Act that applies to everything would make it a more consistent obligation.

Mr. Bob Bratina: I'll make a final quick point. We are trying to remove all the variables through more accurate, if you will, legislation. But the variable factor will always be those people who are holding the information and what they do with it. If you look south of the border again, so I don't have to refer to any north-of-the-border ones, you go from Hoover to Comey and you see all sorts of behaviours that are of interest to the public in this general context.

Mr. Wark, how does the public ever have reassurance that the legislation is drafted properly and that it's in safe hands, other than by having an oversight body?

Mr. Wesley Wark: I think the question of safe hands is critical, Mr. Bratina. I would say that a long study of the history and practices of the Canadian security intelligence community, which goes back decades, indicates that on the whole we conduct security and intelligence practices in a lawful manner and that a culture of lawfulness is actually deeply embedded in the core security and intelligence agencies.

One of the concerns I have about SCISA in that context is that if you draw in agencies from outside of that core that do not have a proper understanding of national security and maybe don't have that culture of lawfulness around complex national security issues, you're going to create problems that otherwise wouldn't be there and don't need to be there.

We have faced scandals in the past and examples of unlawful activity, and no doubt those will occur in the future. But fortunately, in the Canadian context, they're rare in number and I don't think we need to worry about the Canadian security and intelligence community being at heart unlawful or lacking that culture. I think the culture is strong, and, to a certain extent, has been reinforced in Canadian practice by some of the difficult experiences of working, frankly, with the United States as an intelligence partner and ally post-9/11.

Mr. Bob Bratina: Thank you.

[*Translation*]

The Vice-Chair (Mr. Joël Lightbound): I'm sorry, but we're out of time.

Thank you Professor Wark and Mr. Israel for shedding light on these issues.

This concludes our meeting. We'll see each other again next Thursday.

The meeting is adjourned.