HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 034 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, November 17, 2016

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Thursday, November 17, 2016

● (1210)

[*English*]

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

Good afternoon, colleagues and witnesses.

Thank you very much for your patience as we exercise our democratic privileges in the House of Commons in sometimes unforeseen circumstances. I don't think there's anybody at the table who doesn't understand that these things happen from time to time.

Normally I would go through significant formalities at the start of the meeting to introduce you all, but given that we only have about an hour of this meeting left, I think we're going to get straight to it.

This is on the study of the Security of Canada Information Sharing Act, otherwise known as SCISA. We have the Department of Public Safety and Emergency Preparedness, the RCMP, the Canada Border Services Agency, and CSIS here. That will be the order in which your presentations will happen.

We normally allow for up to 10 minutes for presentations. I would encourage you to keep your remarks as brief as possible so that we can get in at least one full round of questioning from the members of the committee.

We'll start with the Department of Public Safety and Emergency Preparedness.

Mr. John Davies (Director General, National Security Policy, Department of Public Safety and Emergency Preparedness): Thank you for the invitation to be here today to discuss the Security of Canada Information Sharing Act, or what we call SCISA. In addition to being a potential recipient of information disclosed under SCISA, Public Safety helps facilitate the use of the act by departments and agencies, and in collaboration with our colleagues at the Department of Justice we played a role in the development of the act.

As you know, the government is reviewing the act to ensure that it furthers collective security while respecting Canadians' rights and freedoms. We believe your study will be most helpful as part of this review process.

[*Translation*]

With my opening remarks, I would like to provide you with background on three areas of significant discussion: what information institutions are authorized to collect, the disclosure threshold, and how the SCISA works as a discretionary authority within the framework of the Privacy Act.

I will conclude by discussing Public Safety Canada's role for the SCISA.

[*English*]

I will briefly outline how SCISA fits into the history of policy on national security information sharing at the federal level. I will try to condense my notes here.

Back in 2004 the Auditor General examined how departments and agencies work together to investigate and counter threats. Then, and again in a follow-up report in 2009, she found that departments and agencies were not sharing intelligence information because of concern with violating provisions of the Privacy Act or the Charter of Rights and Freedoms, whether this concern was valid or not.

There were a number of commissions, and I won't go through the details here: in 2006, Justice O'Connor; in 2010, the commission of inquiry for the bombing of Air India; and finally, in 2011, the government of the day committed to an action on the issue of information sharing in its action plan on Air India flight 182. In 2015 that commitment was fulfilled with the introduction of SCISA.

SCISA permits disclosure of information related to an activity that undermines the security of Canada when the information is relevant to the jurisdiction or responsibility of an institution listed as a potential recipient. Institutions are listed as recipients because of their national security responsibilities, meaning that they could, in accordance with the law, already collect this type of information. The important point to underline here is that SCISA does not change their collection authorities.

As noted, disclosure hinges on whether information relates to an "activity that undermines the security of Canada". This is defined in section 2 of SCISA to include any activity that undermines Canada's sovereignty, security, or territorial integrity, or the lives or the security of the people of Canada. Some activities that could fall within the scope of this definition are also listed in SCISA as examples.

The definition of "activity that undermines the security of Canada" is broader than the definition of "threats to the security of Canada" used in the CSIS Act. SCISA's definition is broader to capture the role not only of CSIS but also of all departments and agencies with a national security jurisdiction or responsibility.

It's important to remember that information can only be shared if it is relevant to the specific jurisdiction or responsibility of the recipient institution within their respective authorities.

As a threshold, “relevant” allows institutions to disclose information when it is linked to the mandate of the recipient institution. “Relevant” also integrates important aspects of responsible information sharing. In particular, to reasonably determine whether information is relevant, the institution must assess whether the information is accurate and reliable.

● (1215)

[*Translation*]

Finally, “relevant” requires that the connection be real and present at the time of disclosure. Information cannot be disclosed on the basis that it is potentially relevant or will likely be relevant at some time in the future.

[*English*]

Lastly, if there is a legal restriction or prohibition on disclosing information, SCISA does not apply.

The Privacy Act includes a general restriction on disclosing personal information without the consent of the related individual. However, as noted in section 8 of the Privacy Act, it also includes a list of situations in which personal information can be disclosed despite this general restriction. For example, personal information may be disclosed for the purpose for which the information was collected. In addition, personal information may be disclosed in accordance with disclosure authorities in other acts of Parliament, such as SCISA.

When they receive information disclosed under SCISA's authorities, as noted in section 4 of the Privacy Act, departments and agencies must still ensure that personal information “relates directly” to an operating program or activity before they collect it.

[*Translation*]

In addition to these requirements, departments and agencies must also continue to abide by government requirements. These include the Treasury Board Directive on Privacy Impact Assessment.

[*English*]

Privacy impact assessments, or PIAs, help institutions ensure they are meeting the Privacy Act obligations. Under the directive, a PIA must be initiated whenever a substantial modification is made to a program or activity. While SCISA has no impact on collection authorities, the way programs or activities collect information under these authorities may change. If there are changes that result in a program or activity being substantially modified, a PIA is required.

While each institution is responsible for how they implement SCISA, Public Safety's role is to help institutions understand the act. To that end, we create guidance on SCISA. We've conducted information sessions for government officials and we released a framework to guide SCISA's implementation. We continue to provide support to government departments and agencies, as required, and are looking to improve the guidance we provide, including addressing the issues raised recently by the Privacy Commissioner in his annual report.

The Minister of Public Safety has also written to his colleagues regarding the importance of completing PIAs when required. Looking forward, the national security consultation launched by the Minister of Public Safety and the Minister of Justice represents an important step forward on Canada's national security framework. The input we are receiving on, for example, how activities under the act are reviewed, the list of potential recipients, and record-keeping of SCISA disclosures is of great value to us as policy advisers to the government.

[*Translation*]

I look forward to discussing this topic with you today and reading the outcomes of your study.

Thank you.

[*English*]

The Chair: Thank you very much, Mr. Davies. I appreciate your keeping that relatively short.

We'll now move to the RCMP.

Ms. Whelan, thank you very much.

Ms. Alison Whelan (Executive Director, Strategic Policy and External Relations, Federal Policing, Royal Canadian Mounted Police): Thank you, and thank you for the invitation to appear before the committee this afternoon.

I'm Alison Whelan, executive director, strategic policy and external relations within the federal policing program of the RCMP. I'm joined today by Chief Superintendent Scott Doran, from federal policing criminal operations at national headquarters.

Our respective groups were responsible for developing the RCMP's position on the Security of Canada Information Sharing Act, or SCISA, and for ensuring the appropriate information-sharing safeguards are in place on coming into force.

Chief Superintendent Doran and I welcome the opportunity to discuss the act and the RCMP's broader collection, retention, and protection of information related to the organization's national security criminal investigations. This includes the personal information of individuals, both Canadians and non-Canadians, identified during the course of national security criminal investigations.

Prior to the implementation of SCISA, the RCMP had broad authority to exchange national security-related information with domestic and foreign partners, consistent with its mandate, relevant laws, ministerial directives, and in accordance with operational policy. The authority to collect, analyze, exchange, and store national security-related personal information is essential in order to build cases and present evidence against those who violate Canadian law and, equally, to exonerate those who are falsely accused.

The RCMP's national security-related information exchanges range from the sharing of intelligence reports on the tactics and techniques of terrorist organizations to conversations between law enforcement agencies on prevention techniques to notification to and from partner agencies about possible national security threats and attack plans, as well as the disclosure of private information about individuals as part of ongoing criminal investigations.

From the outset, the RCMP supported our partners in the development of the Security of Canada Information Sharing Act, recognizing that there were some government departments and agencies lacking the authority or clarity to share relevant information to protect Canada's security.

The RCMP has taken a number of steps to inform our members of the act and to establish procedures for sharing, storing, and tracking disclosures and receipts of information.

Pursuant to subsection 5(1) of SCISA, the RCMP commissioner has delegated the authority to receive information disclosed to a select number of senior positions in the national capital region. In fact, the manner in which the RCMP both discloses and receives information through SCISA is managed at national headquarters. For example, federal policing's intake unit is the main point of contact for proactive disclosures to the RCMP by Government of Canada institutions.

In the context of national security criminal investigations, particularly those related to high-risk travellers and returnees, federal policing criminal operations is responsible for managing all proactive disclosures by the RCMP, requests for information to Government of Canada institutions, and the information received.

On the same day the act came into force, a communiqué was distributed to all criminal operations officers responsible for overseeing federal investigations across the country. The communiqué provided information about the provisions of the act, the list of institutions authorized to receive information under the act, and a list of the RCMP officials with the delegated authority to receive information disclosed pursuant to SCISA.

As noted, the RCMP already had the authority to disclose national security-related information to domestic security and intelligence partners. However, for the purpose of SCISA, any information about an activity that undermines the security of Canada that the RCMP discloses or receives through its designated recipient institution will be documented as a disclosure under the act. All correspondence related to SCISA must be documented in the RCMP's secure records management system as well.

Federal policing has also established processes to maintain statistics on disclosures made to and by the RCMP under the act, including what was disclosed, who disclosed it, and when it was disclosed.

As you're likely aware, the Office of the Privacy Commissioner recently commenced an investigation of the Security of Canada Information Sharing Act under section 37 of the Privacy Act. The RCMP welcomes the review and has provided data to the Office of the Privacy Commissioner regarding how many disclosures we have both received and made under the act during the two time frames of August 1, 2015, to January 30, 2016, and February 1, 2016, to July 31, 2016. Engagement with the Office of the Privacy Commissioner is continuing, with meetings set for later this month between representatives of the review team and the federal policing program.

To date, the majority of the disclosures the RCMP has both made and received have been as part of the activities undertaken by the RCMP national security joint operations centre.

● (1220)

Briefly, the national security joint operations centre, or NSJOC, was established by the RCMP in October 2014 as a venue for facilitating real-time information exchange among key government departments and agencies to help disrupt and prevent terrorism-related travel abroad or to mitigate imminent threats of terrorism-related violence at home.

The national security joint operations centre is essential in supporting the RCMP-led integrated national security enforcement teams. These teams, located in Vancouver, Edmonton, Calgary, Toronto, Ottawa, and Montreal, have primary responsibility for investigating terrorism-related files.

To effectively counter the threat of terrorism, all the capabilities, experience, and powers of the Government of Canada must be brought to bear. The national security joint operations centre facilitates this by bringing together most of our federal partners in one place. Since its inception, several departments and agencies, including the Canadian Security Intelligence Service, the Canada Border Services Agency, and Immigration, Refugees and Citizenship Canada, have been co-located in an RCMP facility in Ottawa to facilitate information sharing and enable a coordinated approach to operational decision-making. I would emphasize that the national security joint operations centre neither replaces nor impedes the member agencies' prerogative to make independent operational decisions consistent with their respective mandates and applicable laws.

The key strength of the centre is expedient information sharing for effective responses. The officer in charge of the national security joint operations centre has been delegated the authority by the RCMP commissioner to receive information disclosed pursuant to SCISA.

The work carried out via the national security joint operations centre is an excellent example of how the powers granted under the Security of Canada Information Sharing Act enable information sharing to be better targeted and expeditious. Prior to SCISA, when the RCMP needed to access information from federal departments or agencies outside the national security and intelligence community, there were disparate systems for information exchanges, and they were often lengthy. In some cases requests could take up to three weeks to process and could include more information than investigators truly needed. SCISA allows the personnel at the national security joint operations centre to exchange information in a more streamlined way. We now use a standardized form, and requests are typically processed within 24 to 48 hours. I must stress that this expediency has not come at the expense of privacy; exchanges continue to be made in writing and on a case-by-case basis.

I will close by noting that the RCMP finds SCISA to be a critical component in the information-sharing authorities we already have.

Thank you, and we welcome your questions.

● (1225)

The Chair: Thank you, Ms. Whelan.

Mr. Mundie, welcome back for your monthly visit to the committee.

Mr. Robert Mundie (Director General and Chief Privacy Officer, Corporate Secretariat, Canada Border Services Agency): This is my third appearance before this committee.

My name is Robert Mundie, as you probably know. I'm the director general of the corporate secretariat and I'm also the chief privacy officer for the Canada Border Services Agency.

Today I'll briefly outline our operating context in general, and then in particular I'll focus on the manner in which information is shared with other government departments, including under the Security of Canada Information Sharing Act, or SCISA.

The CBSA is responsible for border functions related to customs and immigration enforcement, as well as food, plant, and animal inspection.

The agency administers and enforces two principal pieces of legislation in relation to processing people and goods within the border context: the Customs Act, which sets out our responsibilities to collect duties and taxes on imported goods, interdict illegal goods, and administer trade legislation and agreements, and the Immigration and Refugee Protection Act, which governs both the admissibility of people into Canada and the identification, detection, and removal of those deemed to be inadmissible under the act. The agency also administers over 90 statutes on behalf of other federal departments and agencies.

[*Translation*]

Given the numerous daily interactions the agency has with individuals and their goods, as well as our relationship with our Public Safety partners aimed at upholding national security, the CBSA is well-versed in information sharing activities that are both lawful and respectful of personal privacy.

Many of CBSA's business lines engage in information sharing for specific purposes. These can include trade and commercial facilitation, criminal investigations, national security screening, and interdiction of illegally imported or exported goods.

[*English*]

Regardless of the reason, when information is shared, two important conditions apply in all cases.

First, all information sharing must take place in strict accordance with Canadian law. The vast majority of the CBSA's disclosures take place under the auspices of either the Privacy Act, section 8, or the Customs Act, section 107. These provisions are structured as blanket prohibitions against disclosure of information, accompanied by a number of very specific exceptions to this prohibition. The Customs Act has an exception for disclosing customs-related information for national security purposes, for example, while the Privacy Act does not explicitly allow for disclosure for national security reasons. Three provisions of the Privacy Act can, however, be used to disclose national security-related information, but they are either too restrictive or cumbersome to be of timely and practical use.

To illustrate, the “consistent use” provision in paragraph 8(2)(a) of the Privacy Act could be used, but it requires that the information that was exchanged was used for a similar purpose for which it was collected. Given different departmental mandates, this is not always a reliably available provision for us to use.

Designated investigative bodies can also request information under paragraph 8(2)(e), but this requires that they be aware of the need to make a request in the first place, because proactive disclosure is not permitted under this provision of the Privacy Act. Proactive disclosures made for the public interest are also permitted by paragraph 8(2)(m), but the process is cumbersome, requiring an average of 10 days for a disclosure to be approved.

SCISA addresses all of these limitations.

● (1230)

[*Translation*]

The second necessary condition is that the CBSA's information-sharing activities are well governed by policy and by training. Each of the acts mentioned above, including SCISA, has a specific CBSA policy dedicated to information sharing. These policies provide succinct guidance on the assessment of privacy rights, approval levels for each disclosure type, and protection of information, amongst other considerations.

Policy implementation is strongly supported by two well-received online information-sharing training courses, and SCISA was specifically introduced with multiple information sessions in August 2015.

[*English*]

As indicated in the Office of the Privacy Commissioner's report of 2015-16, a review of SCISA-related activities has showed sparing use of the provisions. In the first half of the year of implementation, the CBSA made 24 disclosures under SCISA, and during the same time period, eight disclosures were made to the CBSA.

The agency looks forward to working with all stakeholders in the realm of information sharing and privacy so that we may continue to evolve in the right direction.

In closing, I want to thank you, the committee, for the opportunity to provide our input into your study and for welcoming me here today. I'm happy to answer any questions you may have later.

The Chair: Thank you, Mr. Mundie. It's much appreciated.

We'll now move to CSIS. We have Ms. Tricia Geddes here to bring her remarks.

Ms. Sheppard is here from the Department of Justice, I believe, just to provide answers to questions.

Ms. Ann Sheppard (Senior Legal Counsel, Department of Justice): That's correct.

The Chair: After your remarks, Ms. Geddes, we'll proceed to the round, and we'll start with Mr. Erskine-Smith immediately.

Ms. Geddes, the floor is yours.

Ms. Tricia Geddes (Director General, Policy and Foreign Relations, Canadian Security Intelligence Service): Great. I'm happy to do so. Thank you very much for having me.

First, I'd like to say that I'm offended that I'm not invited as often as my colleague Mr. Mundie here.

Voices: Oh, oh!

Ms. Tricia Geddes: Good afternoon, Mr. Chair and members of the committee. My name is Tricia Geddes, and I am the director general for policy and foreign relations at CSIS. Though my branch encompasses a wide range of functions, most relevant to the issue at hand is our role in the development of policy advice on strategic issues as well as the negotiation arrangements with our partners in support of CSIS's duties and functions. In support of these efforts, my branch has taken a leadership role in supporting the responsible implementation of SCISA.

SCISA, as you know, creates an explicit authority for federal institutions to share information with designated recipients. The sharing of this information must be relevant to activities that undermine the security of Canada. By virtue of CSIS's national security mandate, we are a designated recipient under SCISA.

SCISA sets the threshold for disclosing institutions; it does not change CSIS's mandate. We continue to undertake our duties and functions in accordance with the CSIS Act. Our collection authorities are clearly defined in our act. CSIS is authorized to collect information, to the extent that it is strictly necessary, on activities suspected of constituting a threat to the security of Canada. We may also conduct investigations in the exercise of our security screening mandate.

For the purpose of fulfilling our mandate, threats to the security of Canada are explicitly defined in section 2 of the CSIS Act and are limited to terrorism, espionage, sabotage, and foreign interference. These have remained constant since 1984. CSIS must ensure that any information it collects meets its own legislative requirements, irrespective of the authority relied upon by the disclosing institutions.

● (1235)

[*Translation*]

Effective and responsible sharing of information between government institutions is essential to the common goal of ensuring that Canadians remain safe. Timely access to reliable information is critical to the success of CSIS' lawful investigations. Not only is information essential to identifying and understanding the threats we face, but it also enhances our ability to advise government. CSIS intelligence provides the important insight, it provides situational awareness and informs decision making.

[*English*]

To exercise due diligence, CSIS has adopted a strategic and measured approach to implementing SCISA. CSIS presented its overall approach proactively to the Office of the Privacy Commissioner in the fall of 2015 and has remained engaged with the office on this matter.

As part of its implementation approach, CSIS has worked with key partners to consider the particularities of each relationship and to determine how best to integrate SCISA into the overall relationship. This bilateral approach ensures that all relevant legal policy and operational considerations are assessed with other regimes. Engagement with partners in this regard has occurred on a priority basis that is determined by operational needs and requirements. CSIS and Global Affairs Canada, for example, has signed a new arrangement that governs the sharing of consular information. Whereas our former protocol relied exclusively on the Privacy Act, the new protocol integrates SCISA, filling an important gap, a gap that had been identified by SIRC.

I can confirm that we have received information under the authorities of SCISA in support of active investigations, as noted in the Office of the Privacy Commissioner's 2015-2016 annual report. Information shared during the first six months of SCISA respected the threshold set out in law.

This review is an example of how CSIS' activities can be, and are, reviewed within a broader framework of accountability. The Privacy Commissioner can review CSIS' information-sharing policies and practices and issue public recommendations. CSIS continues to co-operate with the Office of the Privacy Commissioner in the context of its review of SCISA.

[*Translation*]

CSIS' activities are also reviewed by the Security Intelligence Review Committee, or SIRC, which reports to Parliament on our operations. SIRC's findings and recommendations provide valuable feedback and as a result often have a direct impact on policies and practices.

[*English*]

As you are aware, SCISA is also part of the range of issues being examined in the ongoing national security consultations. Though these issues are rightly a question for the public and Parliament to consider, we welcome the discussion and the opportunity to hear from Canadians on these important issues, many of which are at the very heart of what we do.

With that, Mr. Chair, I conclude my remarks.

I know that we all welcome to your comments, observations, and questions.

The Chair: Thank you very much to our witnesses.

We'll proceed now to the seven-minute round of questions.

Mr. Lightbound, I guess, is going to go first.

Mr. Joël Lightbound (Louis-Hébert, Lib.): Yes, Mr. Chair, I will go first with my questions.

I want to thank you all for being here with us.

My first few questions are for the RCMP and Madam Whelan. Could you please describe the process you went through, before SCISA came into force, to obtain information from one of the 17 agencies that are listed in SCISA? You touched upon it in your presentation, but what was the process like, and how troublesome was it for you to obtain information, if at all?

Mr. Scott Doran (Director General, Federal Policing Criminal Operations, Royal Canadian Mounted Police): Mr. Chair, I can answer that question.

The process is different for different agencies. For instance, we have arrangements with CSIS to exchange information, but what Ms. Whelan was referring to, I think, was the process by which we would use the Privacy Act requests under paragraph 8(2)(e). Because the requests were not exclusively dealing with national security issues but were dealing with all sorts of issues that the force may ask of different agencies, they could be cumbersome, and different agencies actually have large offices to deal with those requests coming in. Those are processed, and they can take a long time.

Sometimes what we're dealing with, especially with the high-risk travellers, is that things are unfolding now, and we need answers as quickly as possible to be able to deal with them.

Mr. Joël Lightbound: Under SCISA, the 17 agencies that are listed can volunteer information that is relevant to what is stated as a threat to the security of Canada. When the RCMP, for instance, wants to obtain information that is protected by section 8 of the charter, which states that people have a reasonable expectation of privacy, I gather that the RCMP needs a warrant.

Let's say that information covered by section 8 of the charter is volunteered by another agency. How do you proceed if you receive information that you could only have obtained with a warrant, but it is volunteered to you without a warrant? What do you do with that information?

● (1240)

Mr. Scott Doran: There are a number of ways in which we can get information. If SCISA allows a federal government department to share with us, it's their prerogative as to whether they do or not. If it's outside of the realm of an act of Parliament, then clearly it could be a constitutional issue, in which case we would acquire a warrant.

Depending on the situation that presents itself, I think we would use the legislation that is available to us.

Mr. Joël Lightbound: If I understand it correctly, it means that information you would need a warrant to obtain can be volunteered to you and then used because SCISA allows for it, in a way. That's my problem with SCISA.

Go ahead, Madam Sheppard.

Ms. Ann Sheppard: I have just one point, and this was alluded to earlier on: SCISA does not affect collection. It only deals with disclosure.

If, for example, you need a warrant to collect information, SCISA would not interfere with that. That would prevail in circumstances where it would be required.

Mr. Joël Lightbound: Okay, but of the 17 agencies that are listed, there are many that will collect information for a certain purpose, but that information is used by a law enforcement agency for another purpose, for which they might need to obtain a warrant. That's my point.

If the information has been collected.... For instance, look at the 17 agencies. There are a lot of them. If information is obtained by one of these agencies for a whole different purpose, but one of the law enforcement agencies desires to have that information, or if that information is volunteered to the agency without a warrant.... I'm a little confused as to how that works in terms of whether there's a reasonable expectation of privacy on certain information. Could you enlighten us?

Ms. Ann Sheppard: I think there may be some misunderstanding about the scope of SCISA. SCISA is a disclosure authority only. It does not deal with the use of the information that's collected by a recipient agency or with any downward disclosure of it to another agency. As long as the threshold in SCISA is met—as long as it's relevant to the national security jurisdiction or responsibilities of the recipient institution—it can be disclosed, but it always operates subject to any other law that limits disclosure.

For example, if there was something in the disclosing institution's operating legislation that prevented that, SCISA does not override it. It only deals with disclosure, and the threshold has to be met for disclosure to occur. It's up to the recipient. Whether it's proactively disclosed or by request, they have to make sure that they are authorized to collect it. Nothing changes their existing collection authorities. They may have a very stringent regime. They may need a warrant to collect it. That continues to apply. Also, how they use it has to be within their existing authorities. SCISA doesn't touch that.

Mr. Joël Lightbound: Thank you.

While I have you here, Madam Sheppard, I am looking at section 8 of SCISA in regard to "No civil proceedings". In regard to immunity in the case of fault, do you think that such a provision would have prevented someone like Maher Arar from obtaining compensation?

Ms. Ann Sheppard: Sorry—did you say "section 8"?

Mr. Joël Lightbound: It's section 9 of SCISA. It states:

> No civil proceedings lie against any person for their disclosure in good faith of information under this Act.

Could it have prevented someone like Maher Arar from being compensated?

Ms. Ann Sheppard: I don't really think it pertains to the situation you're talking about.

It's perhaps useful to explain something about this provision. When we decided to include it, we consulted with operating agencies and departments, which revealed that some civil servants were reluctant to lawfully share information because they were afraid they would be found personally liable in terms of committing a criminal act for disclosing information. It was really done to help allay anxiety and to encourage responsible disclosure, charter-compliant disclosure.

The provision is there to inform public servants that they will be protected from civil liability if they disclose information in good faith, and that's why it was included. It shields individuals. It was not ever intended to shield the crown from immunity, and that may be something that people don't understand.

Individuals who are adversely affected by sharing could begin civil liability proceedings against the crown, which could be found vicariously liable for the actions of its employee, but it wouldn't protect them from criminal liability if they maliciously shared information. That's what that provision is for. I just thought I'd explain.

● (1245)

Mr. John Davies: Also, the case you're talking about was about sharing with another government—

Mr. Joël Lightbound: Yes, I know, a foreign one, but—

Mr. John Davies: SCISA is about within the government.

Mr. Joël Lightbound: I understand that completely, but the principles remain that oversharing of information could lead to certain circumstances. I understand the difference, but I think there are some similarities.

Do I still have time?

The Chair: We're past seven minutes, Mr. Lightbound. I apologize, but we need to move on.

Mr. Kelly, you have up to seven minutes, please.

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

Perhaps I might be in some of the same vein with some of my questions.

We've heard from other witnesses in our study about the constant conflict between the necessity of sharing information for the various security and intelligence agencies to be able to do their jobs correctly to protect Canadians, while at the same time continually being aware of the right to privacy that Canadians expect.

Ms. Geddes, we've heard from other witnesses about the importance of both these conflicts, and also with respect to the sharing of information with our Five Eyes partners in particular, as well as with other international partners.

In your view, does SCISA facilitate both these priorities, the priority to be able to make appropriate disclosures of information to protect Canadians and our allies, as well as to maintain Canadians' privacy? Can you comment?

Ms. Tricia Geddes: I'm happy to comment. Thank you for the question.

I believe your question was about whether or not we're striking the right balance with SCISA. Speaking from the services perspective, we had experienced some challenges in information sharing, and SIRC had commented on them. In particular, in one of their reports they focused on our information exchanges with Global Affairs Canada and our ability to receive information from Global Affairs Canada.

That is one area in which I think SCISA has been very helpful to us, for sure. I think that's enhancing national security, absolutely and certainly. I can't speak to any specific investigations, but we have certainly been the beneficiary of information there.

While we had been using the Privacy Act for our information exchanges with Global Affairs before this, now that we have the additional powers or the additional clarity around SCISA, there have certainly been some enhancements there, so I feel confident.

I don't know if your second question was more about how we deal with allies and so on in the current threat environment.

Mr. Pat Kelly: No, I really wanted you to comment specifically on whether SCISA did strike the right balance between the objectives you have for your agency and protecting privacy.

If I may shift a little, perhaps Ms. Sheppard might be the best one to comment on this. I heard more than one presenter repeat an identified concern about individuals who would be reluctant to make a disclosure for fear of violation of privacy law, whether founded or unfounded.

We as a committee, in studying the Privacy Act, have heard from many witnesses about the demands people have for privacy, and yet a failure to communicate important information that results in a crime, perhaps a horrific or catastrophic crime, is of equal concern to Canadians when something like this has happened. Nobody wants ever again to have a commission that looks into how agencies fail to communicate with each other to prevent a crime.

Does SCISA do enough to allay individual concerns that people have over violating privacy law to do their job correctly?

Ms. Ann Sheppard: We've intended to have the provisions developed in a way that meets those goals of both encouraging responsible disclosure and doing so in a charter-compliant way. We have the reference in the preamble to the charter. We have guiding principles that are intended to help guide interpretation and application of the act.

In the end, we did not decide to have a compulsion to share information. We very much had the charter privacy protection in mind there. It's a discretionary authority to disclose. It has to be according to case law and exercised in accordance with the charter. The attempt is to encourage disclosure by having one clear authority that applies to all disclosing institutions, some 200 disclosing institutions, so it's laid over the patchwork of regimes that already existed.

In exercising discretion, the agencies would have to keep in mind the very important national security reasons that their information, if relevant, should be disclosed; however, it's not a rubber-stamp exercise, so in exercising discretion they could also have valid reasons for not sharing it. In developing a one-size-fits-all act, we had to think that there might be impacts on ongoing investigations and things that would mitigate against disclosure. We really tried to put a framework in place that would allow appropriate exercise of discretion in a charter-compliant way and encourage the important national security objectives of the act.

● (1250)

Mr. John Davies: Just to add on that, SCISA has proved to be necessary but non-sufficient, in the sense that other than closing legal gaps and having a clear legal framework from which to encourage departments and agencies to share in the national security agencies, it allows more training, learning, or working on educating people, particularly those in the non-national security world, on how those gaps are closed and how they can use the act in a way that creates safeguards and respect for privacy but also helps on the national security front.

Mr. Pat Kelly: Am I out of time?

The Vice-Chair (Mr. Joël Lightbound): You have 30 seconds.

Mr. Pat Kelly: Then I'll give it back, because I'll probably end up going way over if we ask another question.

The Vice-Chair (Mr. Joël Lightbound): Perfect. That's very wise of you.

Mr. Blaikie is next.

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

My first question has to do with the threshold for sharing. Under SCISA it's that the information has to be "relevant" to identifying a national security threat. My understanding is that the Privacy Commissioner has said that is not a strict enough threshold. He believes that it should be "necessary" for the identification of a security threat.

I'm wondering if we could hear, especially from CSIS and the RCMP, what the operational differences for your organizations would be if you were to switch from a threshold of relevancy to a necessity threshold.

Ms. Tricia Geddes: Do you want me to go first?

Why don't you start, John?

Mr. John Davies: Threshold is absolutely key. You're right to ask and to think about that. If the threshold's too low, there are, obviously, negative privacy impacts. If it's too high, the benefits to national security and the viability of the act are threatened.

In my remarks I just tried to talk a bit about what relevancy means. It implies a test on the discloser, whether that's amongst the 17 or outside the 17, to understand the reliability and the accuracy. It has to be something that's in real time, and it can't be something hypothetical or future or anything. Is it actually meaningful? It exists elsewhere in other acts in terms of an information threshold.

The key thing for the agencies here, but particularly the non-national security agencies, is as you go up and you think about higher thresholds, you think about what that would mean. You're putting other agencies in a position to be experts on the mandate of the agency you're giving the information to, right? That could create problems. It could create internal constraints. To be challenged on that decision later would obviously be awkward for them. They would have to show that they really understood that mandate, that it was required to give that information for that agency to do its job, and that may create problems. It's just something to think about as you ponder the threshold in your work.

Ms. Tricia Geddes: Let me add to that—briefly, because I'll echo exactly what John said.

One concern is that we sometimes are dealing with partners who are not national security experts. In our case in particular, I've been using the example of working with Global Affairs Canada, for instance.

It's difficult. There are consular officials all over the world, and although they are sensitized to national security issues, I don't think any of them would self-purport to be expert on national security. Working with them over the last few months when we've been setting up this protocol to talk about what the national security indicators are that we're looking for, and so on, has been extremely helpful in terms of identifying the types of things we need that would be relevant, but they will never know whether something is absolutely essential. That's why the threshold for us is at an entirely appropriate level, and I think raising it would create some challenges and would put an awful lot of pressure on a consular officer to determine whether such-and-such is relevant or not. I think that would be a very difficult position to put them in.

● (1255)

Mr. Scott Doran: I'll just top that off. The nature of the information itself may sometimes not be self-evident. It's only when you put pieces of information together that the constellation of those pieces will begin to make sense from a national security perspective.

That doesn't necessarily apply to the proactive disclosures, but we may be making a request. When we make a request and we justify the national security issues, we may be after only a birth date or a name or something that in itself is not national security but is needed for the building of the information together.

For it necessarily to be national security-related on its own doesn't account for the collection of information that's available from disparate agencies.

Mr. Daniel Blaikie: At the moment, who determines and how is it determined what is relevant in the appropriate sense, and at what point is there a time when you step back and someone else as an oversight body looks at how you as an agency have been characterizing “relevant” or how the consular offices have been characterizing “relevant” and whether that's an appropriate way of characterizing relevancy?

Mr. John Davies: The governance structure linked in the act is that the deputy head is ultimately accountable, but the deputy head can create a delegated structure within his or her department that would include the necessary training and the other people who have authority, for example, to make determinations or advise internally on what is relevant.

I'm not sure whether you've met or will meet the Privacy Commissioner on this act, but he's already reviewing the act for exactly that kind of question. How does that internal governance structure work? Who has been trained to what level? How is it working for them to make sure it's up to the standard that he thinks is acceptable?

Ms. Tricia Geddes: Just to add to that from the service's perspective, this has happened a number of times. We've had many conversations with the Office of the Privacy Commissioner on this, and it's the sort of discussion we're engaged in on an ongoing basis, because it's something that's critical to our being able to successfully implement SCISA to ensure that we've met that test properly. The discussion is primarily with the Privacy Commissioner, but of course SIRC is also able to take a look at any aspect of it that they would like to look at.

Ms. Alison Whelan: The RCMP has been active in the OPC's investigation. They're coming in, I believe, as early as next week. They're going to look at our disclosures, our requests, and then the files that they are related to.

We are open to that. As I said, we've sent out the communique and have tried to impress upon everyone their obligations under SCISA so that the people who have been delegated by the RCMP commissioner are well aware of their responsibilities and their duties related to the handling of national security-related information.

The Vice-Chair (Mr. Joël Lightbound): You have 30 seconds.

Mr. Daniel Blaikie: I'll imitate Mr. Kelly on that point and cede my time.

The Vice-Chair (Mr. Joël Lightbound): Perfect.

We'll now move to Mr. Erskine-Smith for seven minutes.

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

I want to pick up where my friend left off, on the standard. Obviously you've received information or have requested information under SCISA already. Can you give me an example in which information you have received was useful and added value, but wasn't necessary?

I still want to get at why we can't have a necessity standard. I get that Global Affairs might have a hard time doing it, but if the Privacy Commissioner is saying it, if the academic experts that we've heard have all said we should have a necessity standard, give me a specific example showing why a necessity standard would impede your investigations.

Ms. Tricia Geddes: I so wish I could answer that question, but I can't. Obviously we wouldn't be in a position to describe to you specific instances in which we received information and used it for a national security investigation. I'm sorry that I can't offer you a particular example of when that—

Mr. Nathaniel Erskine-Smith: You don't have to give me the nuts and bolts of it, but give me an example. It could be a generic example of an instance where a necessity standard would impede your investigation.

● (1300)

Mr. John Davies: It doesn't matter whether you get a specific example or not. The point is that if you go up to the necessity standard, then there will more than likely be less information going to the national security agencies. Whether it's example A, B, or C, it doesn't really matter. There's likely to be less information moving. The viability of the act....

You would have to test. You would have to talk to the non-national security agencies that are probably most vulnerable to understanding what national security necessity is for those receiving it.

Mr. Nathaniel Erskine-Smith: Presumably if you make the case for necessity to those bodies, and they in good faith disclose that information, then because we have the provision Ms. Sheppard mentioned, they wouldn't be in the position of worrying too much.

We talked about the review. You mentioned SIRC. Obviously the RCMP has a review body, as well. The Office of the Privacy Commissioner was before us many months ago, and they said they didn't have a whole lot of information with respect to SCISA and the information that had been shared under it.

Now offices are being opened. I appreciate that you're networking with the Office of the Privacy Commissioner. We're well over a year past SCISA being in operation now. When we talk about the review structure, and let's take CBSA as an example, you just have the Office of the Privacy Commissioner as the review body. Would that be fair to say?

Mr. Robert Mundie: It's not entirely fair to say, because many of the decisions that are taken by the agency in the realm of trade and in the realm of immigration are subject to external review by quasi-judicial and independent judicial bodies, for example.

Mr. Nathaniel Erskine-Smith: I mean specifically with SCISA. If information is requested by CBSA or if information is disclosed to CBSA, is the review of the propriety of that sharing done only by the Privacy Commissioner? Who would be reviewing that?

Mr. Robert Mundie: It's the Privacy Commissioner's office, yes.

Mr. Nathaniel Erskine-Smith: The Supreme Court has the Wakeling decision, where the law effectively says that information shared has to be governed by a clear law, there have to be reasonable safeguards, and it has to be done in a reasonable fashion.

Obviously, SCISA is the law. Can someone explain to me what the reasonable safeguards are?

Ms. Ann Sheppard: I think there are a number of them in the act. The compelling national security purpose is important.

SCISA is a very contextual act. It has one operating provision, which is section 5. The rest is context, because it applies to so many institutions. There are a number of features in it that you don't usually see all of in a piece of legislation. There are preambular clauses that speak of the importance of respecting the charter.

What's somewhat unusual are the guiding principles that are in the act.

Mr. Nathaniel Erskine-Smith: Those aren't related. Those aren't proper legal safeguards. For the definition you mentioned, “undermine the security of Canada”, that concept would be the legal safeguard, effectively.

The preamble and guiding principles aren't legal safeguards, as it were. They are not legally enforceable in the same way as the definition “undermine the security of Canada” concept would be.

Ms. Ann Sheppard: Right, but they do help set the context of the act, and the courts would take them into account.

Mr. Nathaniel Erskine-Smith: That's fair. Absolutely.

Ms. Ann Sheppard: The definition, as you point out, is a bit novel, so perhaps people aren't familiar with it, but as it was intended to apply to all institutions and to cover all the mandates of the recipient institutions, and to be evergreen and evolve with threats, it is conceptual. Its opening words are its full extent, as in threat to sovereignty, security, territorial integrity, or the lives or safety of Canadians. Those are all concepts that have a pretty high threshold.

Mr. Nathaniel Erskine-Smith: There's been some—

Ms. Ann Sheppard: That was the idea behind the definition.

Mr. Nathaniel Erskine-Smith: Fair enough. Let's get to that definition, then.

We've had testimony before us calling that definition a radical expansion over and above what is in section 2 of the CSIS Act. We've had testimony proposing and recommending to us that we go back to that definition.

I wonder what you would say to that.

Mr. John Davies: In my opening remarks, I talked about this a bit. The definition in the act is broader. The issue is whether all the other 16 departments and agencies would see themselves within the CSIS Act. As a national security agency, you have to look at whether they could see themselves within the CSIS Act.

Mr. Nathaniel Erskine-Smith: Can you give a specific example of another agency operating under a different definition, and why we needed to expand the definition?

Mr. John Davies: I can only talk to the policy work that was done prior. All of the 17 were requested...in fact, anyone who thought they had a national security responsibility was requested to look at their activities, argue, and get their deputy head and minister to agree that they have a national security responsibility and that this definition that we're working on would fit for them. They had never been asked, so—

● (1305)

Mr. Nathaniel Erskine-Smith: I'm probably out of time but—

The Vice-Chair (Mr. Joël Lightbound): You have 45 seconds.

Mr. Nathaniel Erskine-Smith: Okay.

I would ask with my last remaining time for something in writing to explain to this committee what agencies are operating with different mandates that would necessitate the expansion of that definition from—

Mr. John Davies: That would take a bit of time. That's policy work that we're doing in the context of the national security consultations—

Mr. Nathaniel Erskine-Smith: The consultation was already done.

Mr. John Davies: It's a viable question to ask in the context of the consultations that we're doing, but it's not as easy as a one-week or a two-week reply. It will take a few months.

Mr. Nathaniel Erskine-Smith: Presumably it already ought to have been done, if you expanded the definition in the first place and that was your rationale.

Mr. John Davies: Not necessarily the CSIS Act.

Mr. Nathaniel Erskine-Smith: Fair enough. It was not necessarily the CSIS Act.

Ms. Ann Sheppard: Could I just make a couple of points?

One is that the sources of inspiration were the CSIS Act, and it's meant to cover that, and "a purpose prejudicial to the safety or interest of the State" in section 3 of the Security of Information Act, and the terrorist activity and terrorism offences in the Criminal Code.

Why didn't we cross-reference them? We didn't want to bind the interpretation of other statutes. Also, with the Criminal Code, there was concern that people might have to prove *mens rea* before disclosing, so we didn't.

Some of the things that were included were critical infrastructure, global information infrastructure within the National Defence Act, and the capability of the government to deal with certain spheres of activity such as the financial system security intelligence capability. Some of those things were added in. Not all the recipient institutions have a statutory mandate; some operate under the common law or under a prerogative. To try to codify that would be next to impossible, I think, especially when you get into the area of defence. That's one of the reasons we didn't do that, just to give you a flavour.

Mr. Nathaniel Erskine-Smith: More information would be useful, because when we have experts come to us and say it's a radical expansion, it's a real worry for us not to propose that change. Going back to the CSIS Act, it would be good to have evidence as to why that new definition is a necessary one. I would appreciate any additional information you can provide on that.

The Vice-Chair (Mr. Joël Lightbound): Mr. Erskine-Smith, we are well past seven minutes.

Fellow committee members, I don't know if the witnesses have more time in front of them, but since we were delayed due to the votes in the House, the last round of questions would put us at maybe 25 minutes.

Do you want to continue or do you want to adjourn?

Go ahead, Mr. Kelly.

Mr. Pat Kelly: I think we ought to adjourn.

We've had our day compressed a fair bit with the two votes. I think perhaps our witnesses and other committee members may well have some catching up that they need to do before our next responsibilities in the House.

The Vice-Chair (Mr. Joël Lightbound): Okay.

If it's the committee's will to adjourn, I will accept your will, though I found that very interesting.

I want to thank our witnesses for being here and for the work that you do in protecting our country. We appreciate it greatly.

Have a great day. Thanks for being with us.

This meeting is adjourned.